

CA Service Desk Manager

Guía de administración

r12.5



Esta documentación y todos los programas informáticos de ayuda relacionados (en adelante, "Documentación") se ofrecen exclusivamente con fines informativos, pudiendo CA proceder a su modificación o retirada en cualquier momento.

Queda prohibida la copia, transferencia, reproducción, divulgación, modificación o duplicación de la totalidad o parte de esta Documentación sin el consentimiento previo y por escrito de CA. Esta Documentación es información confidencial, propiedad de CA, y no puede ser divulgada por Vd. ni puede ser utilizada para ningún otro propósito distinto, a menos que haya sido autorizado en virtud de un acuerdo de confidencialidad suscrito aparte entre Vd. y CA.

No obstante lo anterior, si dispone de licencias de los productos informáticos a los que se hace referencia en la Documentación, Vd. puede imprimir un número razonable de copias de la Documentación, exclusivamente para uso interno de Vd. y de sus empleados, uso que deberá guardar relación con dichos productos. En cualquier caso, en dichas copias deberán figurar los avisos e inscripciones relativos a los derechos de autor de CA.

El derecho a realizar copias de la Documentación está sujeto al plazo de vigencia durante el cual la licencia correspondiente a los productos informáticos esté en vigor. En caso de terminarse la licencia por cualquier razón, Vd. es el responsable de certificar por escrito a CA que todas las copias, totales o parciales, de la Documentación, han sido devueltas a CA o, en su caso, destruidas.

EN LA MEDIDA EN QUE LA LEY APLICABLE LO PERMITA, CA PROPORCIONA ESTA DOCUMENTACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO INCLUIDAS, ENTRE OTRAS PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO Y NO INCUMPLIMIENTO. CA NO RESPONDERÁ EN NINGÚN CASO NI ANTE EL USUARIO FINAL NI ANTE NINGÚN TERCERO EN CASOS DE DEMANDAS POR PÉRDIDAS O DAÑOS, DIRECTOS O INDIRECTOS, DERIVADOS DEL USO DE ESTA DOCUMENTACIÓN, INCLUYENDO, ENTRE OTRAS PERO SIN LIMITARSE A ELLAS, LA PÉRDIDA DE BENEFICIOS Y DE INVERSIONES, LA INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL, LA PERDIDA DE PRESTIGIO O DE DATOS, INCLUSO CUANDO CA HUBIERA PODIDO SER ADVERTIDA EXPRESAMENTE DE LA POSIBILIDAD DE DICHA PÉRDIDA O DAÑO.

El uso de cualquier producto informático al que se haga referencia en la documentación se registrará por el acuerdo de licencia aplicable. Los términos de este aviso no modifican, en modo alguno, dicho acuerdo de licencia.

CA es el fabricante de este Documentación.

Esta Documentación presenta "Derechos Restringidos". El uso, la duplicación o la divulgación por parte del gobierno de los Estados Unidos está sujeta a las restricciones establecidas en las secciones 12.212, 52.227-14 y 52.227-19(c)(1) - (2) de FAR y en la sección 252.227-7014(b)(3) de DFARS, según corresponda, o en posteriores.

Copyright © 2010 CA. Todos los derechos reservados. Todas las marcas registradas, nombres comerciales, marcas de servicio y logotipos a los que se haga referencia en la presente documentación pertenecen a sus respectivas compañías

CA Product References

Esta documentación hace referencia a los siguientes productos de CA:

- CA Advantage™ Data Transformer (ADT)
- CA Asset Portfolio Management (CA APM)
- CA CMDB
- CA Business Intelligence
- CA Cohesion® Application Configuration Manager (CA Cohesion ACM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Workload Automation (CA EWA)
- CA IT Process Automation Manager (CA IT PAM)
- CA Management Database (CA MDB)
- CA Management Portal
- CA Network and Systems Management (CA NSM)
- CA Portal
- CA Remote Control Manager (CA RCM)
- CA Service Desk Manager (CA SDM)
- CA Service Management
- CA Siteminder
- CA Software Delivery
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA Wily
- CA Workflow
- Unicenter Asset Portfolio Management (UAPM)

Información de contacto del servicio de Asistencia técnica

Para obtener asistencia técnica en línea, una lista completa de direcciones y el horario de servicio principal, acceda a la sección de Asistencia técnica en la dirección <http://www.ca.com/worldwide>.

Contenido

Capítulo 1: introducción	25
Destinatarios	25
Información indispensable.....	25
Procesos y prácticas recomendadas para la gestión de los servicios	26
 Capítulo 2: Gestión de servidores	 27
Número de servidores	27
Tareas de configuración del servidor	28
Configuración de TCP/IP	29
Cambio de la configuración de un servidor	30
Configuración de ITIL	30
Disciplinas del servicio de ITIL	31
Opciones de la interfaz de empleados y de invitados	32
Notificaciones de elementos de configuración	34
Seguridad del registro de actividades	34
Interfaz PDA.....	36
Inicio de servidores secundarios	37
Inicio del servidor principal.....	38
Estado del servidor	40
Configuración de SSL en Tomcat.....	41
Cómo se implementan los servicios Web de CMDBf	42
Cómo detener un servidor (Windows)	43
Cómo detener un servidor (UNIX)	43
 Capítulo 3: Definición de la estructura empresarial	 45
Cómo definir la estructura de negocio	45
Contactos	46
Grupos	46
Departamentos	46
Ubicaciones	47
Organizaciones	47
Definición de la infraestructura empresarial	48
Orden de definición de objetos.....	48
Familias y clases.....	49
Fabricantes y modelos	49
Estado de servicio	49

Distribuidores y tipos de distribuidores	50
Elementos de configuración	50
Herramientas externas de gestión de activos	51
Asistencia multidepartamental	52
Descripción general del soporte de varios sitios	52
Configuración de un sistema CA Service Desk Manager de varios sitios	54
Multicliente	67
Proveedor de servicio	67
Cómo funciona multicliente	68
Impacto de la interfaz de usuario	75
Impacto de Automatización de soporte	79
Impacto de Gestión del conocimiento	80
Cómo usar la opción multicliente	81

Capítulo 4: Implementación de pólizas 93

Implementación de pólizas	93
Notificaciones	93
Asociaciones de actividades	94
Notificaciones de actividades	95
Notificaciones a contactos de objetos	96
Métodos de notificación	98
Notificaciones por correo electrónico	101
Reglas de notificación	105
Ejemplo: creación de una plantilla de mensajes	116
Artefactos en mensajes	118
Frases y códigos de notificación	118
Lista de destinatarios de notificación manual	122
Notificaciones de asignatario anteriores	123
Notificaciones de elementos de configuración	126
Notificaciones de encuestas	128
Cómo agregar hipervínculos de URL a las notificaciones	129
Lector del registro de notificaciones	129
Administración de correo electrónico	133
Buzones de correo	134
Reglas de buzón de correo	135
Políticas de buzón de correo	141
Cómo implementar los buzones de correo	143
Varios buzones de correo	148
Cómo configurar respuestas de correo electrónico	150
Artefactos	153
Consideraciones de uso del artefacto	154
Seguridad y protección del artefacto	155

Acuerdos de nivel de servicio	157
Uso de acuerdos de nivel de servicio	157
<Procesamiento clásico de acuerdos de nivel de servicio>	158
Tipos de servicios y eventos	159
Cómo implementar los tipos de servicio	159
Tipos de servicio predefinidos	160
Configuración de eventos	162
Objetivos del servicio	163
Contratos de servicio	164
Migración de contratos de servicio	166
Hora de infracción	166
Zonas horarias y turnos	167
Seguridad	171
Configuraciones de la base de usuarios de CA EEM y CA Workflow	171
Consideraciones sobre seguridad	181
Autenticación de CA EEM para CA IT PAM	182
Autenticación de usuarios	183
Cómo realiza CA Service Desk Manager la autenticación de usuarios	183
Autenticación externa	184
Tipos de validación	185
Recuentos de usuarios con licencia y conectados	186
Registros internos	186
Integración de CA Service Desk Manager	187
Asociaciones de partición de datos	187
Particiones de datos	187
Configuración de particiones de datos	188
Especificaciones de las restricciones	189
Tipos de restricciones	190
Creación de restricciones de partición de datos para asignaciones de CAB	192
Configuración de restricciones para la partición de datos de Gestión del conocimiento para permisos basados en roles	193
Encuestas	194
Configuración del sistema para incluir estudios	194
Preparación de estudios	194
Definición de notificaciones de encuesta	195
Generación de informes sobre estudios	196
Encuesta gestionada	196
Servicios Web	197

Capítulo 5: Configuración de cuentas de usuario 199

Contactos	199
Definiciones de contactos	200

Grupos.....	201
Tipos de contactos.....	202
Determinación del comportamiento según los tipos de contactos	202
Configuración de notificaciones según el tipo de contacto	202
Selección de contactos según los tipos de contactos	202
Tipos de tratamientos especiales	203
Cómo configurar contactos de tratamiento especial	204
Cómo asociar un contacto a un tipo de tratamiento especial	205
Datos del directorio LDAP	206
Configuración de las opciones de LDAP	207
Verificación de la integración de LDAP	210
Creación automática de un contacto.....	212
Asignaciones del tipo de acceso de los grupos LDAP	213
Importación por lotes de contactos mediante datos LDAP	213
Actualización por lotes de contactos mediante datos LDAP	217
Autenticación LDAP	219
Transport Layer Security (seguridad de la capa de transporte)	220
Asignación de atributos	220
Solución de problemas	222

Capítulo 6: Gestión de roles 233

Funciones	233
Roles predefinidos	233
Seguridad basada en roles	236
Cómo funcionan los tipos de acceso	236
Registros de rol	239
Áreas de acceso funcional	240
Particiones de datos.....	245
Navegación basada en roles	245
Fichas	245
Fichas predefinidas	247
Formularios Web	249
Grupos de formularios.....	249
Árboles de menús.....	250
Recursos de los árboles de menús	251
Barras de menús.....	251
Barras de herramientas	253
Ir a Recursos	253
Conjuntos de ayudas	254
Cómo implementar un rol personalizado.....	254
Cómo implementar un árbol de menús personalizado	256
Creación de un registro de rol	257

Creación de un registro de ficha	258
Creación de un registro de barra de menús	259
Creación de registros de formularios Web	260
Cómo copiar árboles de menús	261
Cómo crear y personalizar un árbol de menús	262
Creación y publicación de un conjunto de ayuda	264
Cambio de roles	265

Capítulo 7: Establecimiento de la estructura de soporte - CA **267**

Estructura de soporte	267
Modelos	268
Modelo interno	268
Modelo externo	269
Modelo combinado	270
CA Workflow	271
Workflow en tiempo de ejecución	272
Selección de definiciones de procesos de workflow	272
Tareas de workflow	274
Integración del workflow de CA IT PAM	274
Componentes de CA IT PAM	275
Integración de CA IT PAM con CA Service Desk Manager en tiempo de ejecución	276
Cómo crear una definición de proceso	277
Creación de formularios de solicitud de inicio	278
Adjuntar una definición de proceso de CA IT PAM	280
Códigos compartidos	281
Códigos de prioridad	282
Códigos de gravedad	282
Códigos de impacto	283
Códigos de urgencia	283
Códigos de estado	284
Códigos de estado de solicitud	285
Códigos de estado de orden de cambios	286
Códigos de estado de incidencia	287
Códigos de estado de tarea	288
Tipos de tareas	289
Seguimiento de incidentes	290
Instalación de seguimiento de incidentes	291
Área de solicitud/incidente/problema	292
Propiedades del área de solicitud/incidente/problema	293
Definición de áreas de petición/incidente/problema para el autoservicio	295
Orden de cambio y categorías de incidencia	295
Categorías de cambio predefinidas	297

Categorías de incidencia predefinidas	297
Reglas para cambiar las categorías en los partes	297
Propiedades de la categoría	298
Definición de cambio y emisión de categorías para el autoservicio	301
Cierre automático de tickets	302
Cómo establecer las definiciones de ticket de cierre automático	303
Cómo definir una notificación de actividad de cierre automático	304
Actividades del ticket relacionado	305
Cómo definir notificaciones de actividad para tickets relacionados	306
Cómo definir notificaciones de actividad de tickets relacionados	307
Cálculo de prioridad	307
Cómo gestiona el cálculo de prioridad los valores de ticket	308
Cómo establecer el cálculo de prioridad	311
Controles de atributo dependiente y transiciones de estado	323
Cómo trabajar con transiciones de estado y controles de atributo dependiente	325
Configuración de transiciones de estado	325
Configuración de controles de atributo dependiente	327
Métodos de servicios Web	328
Flujos de transición predefinidos	329
Procedimiento recomendado: transiciones de estado predefinidas	333
Transiciones de estado para el autoservicio	336
Cómo funcionan las transiciones para autoservicio	337
Cómo crear o actualizar tipos de transición para transiciones	338
Cómo vincular tipos de transición con transiciones	338
Tipos de transiciones predefinidas	339
Temporizadores	341
Zonas horarias	341
Desencadenantes de eventos de tipo de servicio	342
Cómo se utiliza una zona horaria	343
Cómo determinar la zona horaria que se va a utilizar	343
Adjuntos de archivos	344
Carga y descarga de archivos adjuntos	345
Repositorios	346
Anuncios	349
Visibilidad interna del anuncio	350
Especificación de la urgencia del anuncio	350
Configuración de consultas almacenadas	351
Números de secuencias	352
Uso de registros de auditoría	353
Integración con CA Network and Systems Management	353

Capítulo 8: Control del comportamiento del sistema 355

Uso del Gestor de opciones	355
Cómo modificar el entorno del sistema	356
Eventos	357
Macros	357
Tipos de macros	358
Uso de macros con eventos	359
Uso de macros en el comportamiento de las categorías de cambios e incidencias	359
Uso de macros con Notificación múltiple	360
Uso de macros con una condición definida por el sitio	361

Capítulo 9: Configuración de la interfaz Web 363

Configuración de la interfaz Web	363
Funcionamiento de la interfaz Web	364
WebDirector y distribución de la carga Web	364
Web.cfg y CA Service Desk Manager	365
Asignación de motores Web a un WebDirector	366
Definición del rol de los motores Web según los parámetros de WebDirector	367
Entorno no SSL con equilibrio de carga básico	367
Entorno SSL global con equilibrio de carga básico	368
Inicio de sesión en entorno no SSL con equilibrio de carga opcional	368
Inicio de sesión SSL en entorno mixto con equilibrio de carga opcional	369
WebDirector y configuración de motores Web	369
Cómo implementar un entorno de inicio de sesión SSL con un servidor primario solamente ...	371
Creación de sistemas sólo con servidores primarios	371
Comprobación de los valores de parámetro de WebDirector	374
Comprobación del entorno de inicio de sesión SSL	375
Capacidades Web y servidores secundarios	376
Cómo preparar capacidades Web	376
Creación de sistemas con servidores secundarios	377
Configuración del servidor	379
Introducción de cambios mediante pdm_edit.pl	392
Inicio de WebDirector	397
Cómo gestiona WebDirector las sesiones de usuario	398
Mejora del funcionamiento con el almacenamiento en caché de los exploradores	400
Configuración de Microsoft Internet Information Server	400
Configuración de Apache	401
Borrado de cachés	402
Comportamiento de bloqueo de registros en la interfaz Web	403
Impresión de páginas Web de CA Service Desk Manager	404
Modificación del archivo de configuración	404

SchedExpMaximum	413
SelListCacheExclude	414
SelListCacheMax	414

Capítulo 10: Configuración de la asignación automática 419

Asignación automática	419
Relaciones de asignación automática	420
Métodos de asignación automática	420
Cómo empezar a implementar la asignación automática	421
Áreas y categorías	421
Grupos de analista	422
Analistas	423
Asignación automática por ubicación	423
Asignación automática por turno	424
Grupo predeterminado y asignatario	426
Activación de la asignación automática	427
Sustitución con la asignación automática	428
Controles de asignación	429
Asignación manual	429
Opción Assignee_set	429
Opción Iss_assignee_set	429
Area_Defaults	430
Opciones de obligatoriedad de asignatario y grupo	430
Plantillas	431
Interfaz de CA Network and Systems Management	432
Registro de actividades	432
Seguimiento de asignación automática	432
Consultas almacenadas	433
Cómo asigna tickets la función Asignación automática	433
Cómo asigna tareas de workflow la función Asignación automática	440
Asignaciones automáticas basadas en el elemento de configuración	443
Cómo funciona la asignación automática basada en el elemento de configuración	443
Habilitación de asignaciones automáticas basadas en el elemento de configuración	445

Capítulo 11: Gestión de su base de datos 447

Utilidades de la gestión de base de datos	447
Selección y configuración de la base de datos	447
Cargador de bases de datos	448
Cómo crear y utilizar un archivo de entrada	449
Anulación y restauración de restricciones	450
Copia de seguridad de la base de datos	451

Restauración de la base de datos	451
Reemplazo de la tabla de base de datos	452
Extracción de datos	452
Uso de la utilidad de extracción de datos en UNIX	453
Selección de datos para la extracción	453
Anulación de referencias a datos	454
Ejemplo de cómo utilizar pdm_deref	455
Modo dbadmin	457
Reglas de archivado y borrado definitivo	458
Ejecución de reglas de archivado y borrado definitivo	459
Visualización de reglas de archivado y borrado definitivo	460
Inicio del archivado y borrado definitivo mediante programadores de terceros	461
Definiciones de reglas de archivado y borrado definitivo	461
Historial de archivado y borrado definitivo	464
Gestión de adjuntos (arcpur)	466
Cómo restaurar datos archivados	467
Archivado y borrado definitivo de datos de KPI	468
Foros de Gestión del conocimiento de archivado y borrado definitivo	470
Archivado y borrado definitivo con FAST ESP	471

Capítulo 12: Uso del API de texto 473

API de texto	473
Interfaz de línea de comandos	473
Interfaz de CA Network and Systems Management	474
Formato de entrada	474
Palabras clave	476
Convenciones de entrada de palabra clave	478
Cómo dar formato a un mensaje de correo electrónico para actualizar un ticket	479
Inicio y finalización de delimitadores de mensaje de correo electrónico	479
Cómo utiliza artefactos el API del texto	480
Cómo configurar respuestas de notificación para actualizar tickets	481
Métodos de conversión	485
El archivo de configuración	487
Opciones	488
Valores predeterminados	488
Omisión de entradas	489
Entrada de ejemplo	489

Capítulo 13: Cómo gestionar el control de versión 491

Cómo funciona el control de versiones	491
Archivos de control de versión	492

Archivos de control del servidor primario	492
Archivos de control de cliente y de servidor secundario	493
Control de versión para personalizaciones de instalaciones	493
Modos de los servidores para el control de versión	494
Sintaxis de los archivos de control de versión	496
Parámetros de control de versiones	496
Anulación del control de componentes	501

Capítulo 14: Gestión de elementos de configuración 503

Uso de la interfaz Web	503
Visualización de los elementos de configuración	504
Creación de un elemento de configuración	504
Actualización de un elemento de configuración	505
Cómo asociar una ventana de mantenimiento con un CI	506
Visualización de ventanas asociadas para el cambio	506
Visualización del historial de elementos de configuración	507
Desactivación de un elemento de configuración	507
Reactivación de un elemento de configuración	508
Elementos de configuración de Contacto, Ubicación y Organización	508
Creación de un CI para un objeto base	508
Selección de un objeto base para un CI	509
Edición de los detalles de un CI para un objeto base	510
Edición de atributos de CI para un objeto base	510
Creación de un CI de objeto base mediante GRLoader	511
Relaciones CI	511
Tipos de relación entre elementos de configuración	512
Creación de un tipo de relación	513
Gestión de relaciones de CI	514
Creación de relaciones de CI	514
Visualización de las relaciones de un CI	515
Desactivación de relaciones de CI	515
Reactivación de relaciones de CI	516
Desactivación de relaciones de CI (Editar en lista)	516
Desactivación de una relación CI mediante GRLoader	517
Reactivación de una relación CI mediante GRLoader	518
Supresión de una relación de CI de la base de datos	519
Comparación e historial de relaciones de CI	519
Control de versiones	520
Usos del control de versiones	521
Registros de activos compartidos y de seguimiento de auditoría de CI	522
Terminología del control de versiones	523
Orígenes de datos del control de versiones	526

Change Management Integration de CA SDM	527
Integración de CA APM	528
Gestión de control de versiones de CI	529
Gestión de cambios de CA SDM	547
Visualización de los atributos de un elemento de configuración en otros productos de CA	548
Uso del Visor de CMDBf	549
Visualizador CMDB	549
Cómo realizar análisis de causa raíz	551
Administración del visualizador	552
Cómo agregar un activo detectado	553
Indicadores de activo y de CI	554
Conciliación de elementos de configuración	555
Reconciliación basada en MDR	556
Identificación y resolución de CI ambiguos	558
Revisión y modificación de datos de entrada con el área de trabajo de transacciones (ATT) ...	570
Gestión de transacciones guardadas en almacenamiento intermedio	576
Área de trabajo de la transacción	577
Rellenar el área de trabajo de la transacción	579
Cómo utilizar la interfaz Web para actualizar datos en el ATT	591
Gestionar transacciones de relaciones	594
Cómo cargar transacciones en el CMDB	595
Administración del ATT	597
Mantenimiento de datos de CA CMDB	602
Estructura de clases/familias de CA CMDB	602
Cambio de la familia/clase de un único CI	603
Cambio de la familia/clase de una lista de elementos de configuración	603
Cambio de la familia/clase de elemento de configuración mediante GRLoader	604
Ampliación de CA CMDB	605

Capítulo 15: Administración de MDR 617

¿Qué es un MDR?	617
Clases MDR y nombres MDR	618
Cómo complementa un MDR a CA Service Desk Manager	618
Definición de MDR para CA Service Desk Manager	619
Lanzador MDR	619
Definición de una URL para iniciar un MDR	620
Configuración de un proveedor MDR de CA APM	622
Inicio en contexto desde CA CMDB para CA APM	623
Propiedades de CI que admiten la federación de MDR	623
ID del activo federado	623
Nombre MDR	624
Clase MDR:	624

Definición de MDR con la instalación de CA Cohesion ACM	625
MDR de CA Cohesion ACM	626
Cómo se asocia un MDR a un CI manualmente	627
Importación automática de CA Cohesion	628
Asignación de un CI al MDR	628
Administración de definición de MDR	629
Informe de CA Cohesion ACM	630
Importación de CI a CA CMDB mediante GRLoader	630
Restricciones y convenciones de nomenclatura de los elementos de información	631
Convención de nomenclatura system_name	632
Uso del Visor de CMDBf	633
Cómo actualizar archivos de metadatos para la asignación de CMDBf	634
Cómo mostrar valores de atributo de MDR con nombres de atributo de CA CMDB	635
Cómo ocultar atributos de proveedor de MDR	636
Cómo definir atributos de MDR sin equivalentes de CA CMDB	637
Definición de metadatos de proveedores de datos de CMDBf	637

Capítulo 16: Cómo gestionar el cambio 639

Gestión de Cambios de CA Service Desk Manager	639
Componentes de gestión de cambios	640
Visualización del calendario de cambios	641
Responsabilidades de CAB	642
Funcionamiento de procesos de CAB	642
Responsabilidades del gestor de cambios	643
Funcionamiento del rol del gestor de cambios	643
Definición de tareas para el rol del gestor de cambios	644
Categorías de cambios, estado y niveles de riesgo	645
Visualización del panel de resultados de órdenes de cambio	646
Definición de consultas almacenadas de órdenes de cambio	647
Configuración de las opciones del gestor de cambios	648
Calendario de cambios	649
Cómo agregar información de programación a una orden de cambio	649
Plantillas de eventos de iCalendar	650
Exportación de programaciones a iCalendar	651
Vistas de programación	652
Programación de la configuración de vista	654
Cómo programar órdenes de cambio	662
Uso del ejemplo del programador de cambios	663
Cómo programar ventanas para el cambio	667
Visualización de ventanas para el cambio	668
Cómo asociar un CI con una ventana de mantenimiento	669
Visualización de elementos de configuración asociados	669

Creación de un ejemplo de ventana de desactivación	670
Creación de una ventana de mantenimiento global	671
Detección de colisiones y análisis del conflicto	671
Visualización de CA Workflow	672
Cómo visualizar el workflow	672
Definición de proceso de gestión de cambios para CA Workflow	674
Componentes de la definición de proceso de gestión de cambios	675
Cómo instalar la definición del proceso de gestión de cambios	676
Funcionamiento de la definición del proceso de gestión de cambios	682
No se encontró el actor ActivityNode: actualice el objeto -Service Desk r12	692
No se cierra la orden de cambio	693
Generación de informes y Consola de CAB	693
Gestionar los grupos de CAB	694
Asignación de grupos de CAB	696
Aprobaciones de CAB	696
Modificación de las propiedades de la Consola de CAB	696
Informe de gestión de cambios	698
Evaluación de riesgos	699
Cómo implementar la encuesta sobre riesgos	699
Cómo acceder a una encuesta de riesgos directamente desde una URL	701
Explorador de impactos	702
Inicio de Explorador de impactos	703
Exploración de los elementos de configuración adjuntos	703
Visualización de elementos de configuración en Explorador de impactos	704
Cómo agregar un elemento de configuración relacionado a una orden de cambio	705
Cómo mostrar la lista de descendientes de elementos de configuración	705
Inicio del Visualizador de CMDB desde Explorador de impactos	706
Configuración de Explorador de impactos	706

Capítulo 17: Gestión de informes de CA Business Intelligence 709

Informes de CA Business Intelligence	709
Escenarios de generación de informes	710
Componentes de los informes	711
Diagrama de flujo de datos de informes	713
Visualización de informes en InfoView	714
Seguridad y autorización	714
Grupos y usuarios	715
Universo y conexiones de universos	715
Carpetas de informes	716
Niveles de acceso	718
Cómo dirigir un servidor existente de CA Business Intelligence a un servidor de CA Service Desk Manager	719

Creación de una fuente de datos ODBC	719
Configuración del universo.	721
Exportación del universo	721
Cómo configurar la seguridad de partición de datos para la generación de informes	722
Adición de un usuario con privilegios de CA Service Desk Manager a CMC.....	723
Definición de las credenciales de la base de datos de universo	723
Establecimiento de particiones de datos	724
Base de datos replicada para la generación de informes sin conexión	724
Informes de Role-Based.....	725
Definición de informes de Role-Based	725
Mostrar nuevos informes en la ficha Informes.....	727
Informes basados en Web	734
Interfaz de BusinessObjects InfoView	735
Desplazamiento por los informes.....	735
Preferencias de InfoView	736
Programación de informes.....	736
Configuración de análisis de datos	737
Publicación y distribución de informes	737
Informes de cuadros de mandos	738
Visualización de informes de cuadros de mandos operativos	739
Informes ad hoc	739
Interfaz de Web Intelligence	740
Cómo funcionan los informes ad hoc	740
Informes ad hoc de ejemplo	741
Indicadores clave de rendimiento	747
KPI Types	747
KPI predefinidos	748
Daemon de KPI	748
KPIs de sistema	749
KPI de consultas almacenadas	751
KPI SQL	751
Campos KPI	753
Recuperación de datos del ticket	754
Solución de problemas	757
Escritura de informes de CA Business Intelligence	759
Controlador ODBC de CA Service Desk Manager	759
Escribir SQL para informes de BusinessObjects	760
Funciones PDM	761
Alias de atributo	764
SQL interactivo de pdm_isql	764

Capítulo 18: Generación de informes en CA Service Desk Manager 767

Generación de informes	767
Vistas de las bases de datos	767
Vistas básicas	768
Vistas avanzadas	770
Configuración de métodos de generación de informes	771
Formato de informes	771
Modificación del orden de clasificación de columnas	772
Informes de resumen y detalles	772
Informes de análisis	773
Generación de informes de solicitudes o incidencias	773
Generación de informes de áreas de solicitud o categorías de incidencias	774
Generación de informes de prioridad de áreas de solicitud o prioridad de categorías de incidencias	774

Capítulo 19: Gestión de conocimiento 775

Gestión del conocimiento	775
Búsqueda de procedimientos para la gestión de conocimiento	776
Conocimiento y multicliente	776
Cómo configurar una base de conocimiento	777
Importación de datos de conocimiento de muestra	778
Control de la base de conocimiento	778
Reindización de la base de conocimiento	778
Reindización y desindización de la configuración de colas para procesamiento instantáneo y por lotes	779
Cómo utilizar documentos en la base de conocimiento	780
Envío de conocimiento desde CA Service Desk Manager	782
Envío de conocimiento desde el autoservicio	782
Atributos de Documento	783
Permisos del documento	783
Edición de resoluciones	783
Preparación de la publicación del documento	784
Publicación del documento	785
Control de versiones de documentos	785
Vencimiento de documentos	786
Archivado y borrado definitivo de documentos	786
Archivos de conocimiento	786
Búsqueda de conocimientos	787
Foros	788
Documentos de árbol de conocimientos	788
Programación de documentos de conocimiento	789
Filtro de programación del conocimiento	789

Vistas de programación de conocimiento	792
Programación de la configuración de vista	793
Acceso a exportación/importación	799
Cómo exportar o importar conocimiento	800
Exportación e importación de documentos	803
Paquetes de exportación/importación	803
Visualización de plantillas de exportación/importación	805
Herramienta de exportación de conocimiento de utilidad de pdm_ket.....	811
Utilidad pdm_kit: herramienta de importación de conocimiento	812
Cómo permitir a los usuarios exportar e importar conocimiento	814
Servicios Web	814

Capítulo 20: Administración de Gestión del conocimiento 815

Administración de conocimientos	815
Búsqueda de procedimientos para la administración de conocimiento	816
Funciones y roles de Gestión del conocimiento.....	816
Interfaces de usuario de Gestión del conocimiento	818
Funciones de gestión y configuración de Gestión del conocimiento	818
Opciones de conocimiento de autoservicio	819
Documentos y usuarios	825
Cómo gestionar los privilegios de rol y la visibilidad del documento	829
Contenido de acción	830
Visualización de contenido de acción	831
Creación de contenido de acción (URL de la acción)	832
Creación de contenido de acción (HTMPL interno)	833
Edición de contenido de acción.....	833
Búsqueda de contenido de acción	834
Proceso de aprobación del documento	835
Gestor de procesos de aprobación	836
Definición de un proceso de aprobación para la edición de documentos	837
Creación de plantillas de proceso de aprobación	838
Definiciones de estado del documento	841
Políticas automatizadas	842
Visualización de políticas automatizadas.....	843
Cómo configurar políticas automatizadas	844
Creación de una política automatizada	845
Edición de una política automatizada	846
Programación de políticas automatizadas	846
Visualización de informes de políticas de ciclo de vida de los documentos	847
Control del documento de conocimiento	847
Tipos de comentarios	848
Plantillas de documento	853

Cómo crear vínculos de documentos de conocimiento	861
Categorías de conocimientos	863
Creación de categorías del conocimiento	864
Modificación de categorías	867
Eliminación de categorías	868
Cómo mover una categoría	869
Copiar categorías con vínculos de documentos	870
Copiar categorías sin vínculos de documentos	871
Gestión de permisos de categorías	871
Informes y métricas	873
Tarjeta de informes de conocimientos	873
Informes basados en Web	875
Formularios Web de informes basados en roles	875
Búsqueda	875
Motor de búsqueda de KT	876
Búsqueda FAST ESP	889
Documentos recomendados	892
Configuración de los valores de búsqueda predeterminados	896
Opciones de integración de CA Service Desk Manager	898
Definición de asignación de campos	899
Definición de la configuración de búsqueda de incidencias	902
Definición de la configuración de búsqueda de solicitudes/incidentes/problemas	903
Sugerencias de conocimiento	904
Definición de categorías de incidencia	904
Definición de áreas de solicitud/incidente/problema	905
Configuración de políticas de autoservicio	907
Solution Survey	907
Definición de valores de preguntas frecuentes	908
Definición de los valores de la encuesta de soluciones	910
Configuración del sistema de Gestión del conocimiento	910
Configuración de los valores generales	911

Capítulo 21: Administración de Automatización de soporte 913

Automatización el soporte en el entorno	913
Asistencia en vivo	913
Administración del analista de Automatización de soporte	916
Modo en el que los analistas inician la asistencia en vivo	917
Cómo configurar la asistencia en vivo para analistas	919
Modo en el que los usuarios finales se unen a las sesiones de asistencia	920
Modo en el que los analistas automatizan el soporte para los usuarios finales	921
Modo en el que los analistas proporcionan la asistencia en vivo	921
Administración de usuarios de Automatización de soporte	922

Cómo configurar los permisos de rol de Automatización de soporte	923
Usuarios registrados y anónimos de Automatización de soporte	924
Cómo configurar Automatización de soporte para los usuarios invitados	924
Administración de nivel de acceso de Automatización de soporte	926
Administración de notificación de actividades de Automatización de soporte	927
Adaptaciones de página de Automatización de soporte	928
Administración de personalizaciones	929
Administración de localización	929
Configuración de diseño de página	930
Propiedades del sistema de Automatización de soporte	931
Administración de colas de Automatización de soporte	931
Gestión de colas	932
Cómo gestionar resúmenes de cola	933
Cómo gestionar las horas de la cola	933
Gestión de plantillas de tickets	934
Valores de administración	934
Cómo configurar los valores de Automatización de soporte	934
Cómo personalizar las herramientas de Automatización de soporte	936
Tareas automatizadas	937
Administración de conversación preestablecida	942
Credenciales predeterminadas	943
Cláusulas de exención de responsabilidad	944
Administración del registro de sesión	944
Visualizar el registro de sesión	944
Informes de Automatización de soporte	945

Apéndice A: Descripciones de los campos de vista 947

Descripciones de los campos de vista	948
View_Act_Log	948
View_Audit_Assignee	950
View_Audit_Group	950
View_Audit_Priority	951
View_Audit_Status	952
View_Change_Act_Log	952
View_Change	954
View_Change_to_Assets	959
View_Change_to_Change_Act_Log	959
View_Change_to_Change_WF	961
View_Change_to_Properties	963
View_Contact_Full	964
View_Contact_to_Environment	967
View_Group	968

View_Group_To_Contact	969
View_Issue	969
View_Issue_Act_Log	974
View_Issue_to_Assets	975
View_Issue_to_Issue_Act_Log	976
View_Change_to_Requests	977
View_Issue_to_Issue_WF	981
View_Issue_to_Properties	983
View_Request	984
View_Request_to_Act_Log	989
View_Request_to_Properties	990

Apéndice B: RFC 2251: códigos de resultados de LDAP 991

Códigos devueltos de LDAP	991
Códigos devueltos de servidores LDAP	991
Códigos devueltos de clientes LDAP	997
Estándares RFC asociados a LDAP	999

Apéndice C: Comandos de referencia 1003

bop_sinfo: mostrar información del sistema	1004
dbmonitor_nxd: daemon de control de base de datos	1005
pdm_backup: escritura de bases de datos en archivos ASCII	1007
pdm_cache_refresh: actualización de bases de datos	1008
pdm_configure: apertura de la ventana de configuración	1010
pdm_d_refresh: inicio de demonios erróneos	1010
pdm_deref: anulación de referencias de datos ASCII	1011
pdm_discimp: importación de activos detectados	1015
pdm_discupd: actualización de activos detectados	1017
pdm_edit: configuración de procesos de servidor	1017
pdm_extract: extracción de datos de las bases de datos	1019
pdm_halt: finalización de demonios o detención de servicios	1023
pdm_init: inicio de demonios	1023
pdm_key_refresh: actualización de información de claves almacenada en caché	1024
pdm_lexutil: modificación de léxicos de CA Service Desk Manager	1024
pdm_k_reindex: utilidad de reindexación de conocimientos	1025
Cuándo utilizar pdm_k_reindex	1026
Seguimiento de reindexación	1027
Importación y reindexación	1028
Utilice pdm_k_reindex con FAST ESP	1028
Reindexación y desindexación de la configuración de colas para procesamiento instantáneo y por lotes	1030

pdm_listconn: enumeración de conexiones activas	1031
pdm_load: adición, actualización y eliminación de registros de las bases de datos	1034
pdm_logfile: cambio del tamaño de corte de stdlog	1036
pdm_proctor_init: inicio del supervisor en servidores secundarios	1037
pdm_replace: reemplazo de tablas de bases de datos	1037
pdm_restore: restauración de bases de datos	1039
pdm_status: visualización del estado de demonios o procesos	1041
pdm_task: definición de variables de entorno	1041
pdm_text_cmd: interfaz de la línea de comandos de Text API	1042
Ejemplos de entrada	1044
pdm_uconv--Conversión de un conjunto de caracteres local a UTF-8	1045
pdm_userload: adición, actualización y eliminación de registros de las bases de datos	1048
pdm_webstat: devolución de estadísticas de uso Web	1051
report: generación de informes	1055
rpt_srv: generación de informes	1056
uniconv: inicio de daemon de conversor de eventos de CA NSM en UNIX	1058

Apéndice D: Grupos de formularios **1059**

Grupo de formularios de cliente	1059
Grupo de formularios de empleado	1060
Grupo de formularios de analista	1062

Capítulo 1: introducción

Esta sección contiene los siguientes temas:

[Destinatarios](#) (en la página 25)

[Información indispensable](#) (en la página 25)

[Procesos y prácticas recomendadas para la gestión de los servicios](#) (en la página 26)

Destinatarios

Esta guía está destinada al administrador de CA Service Desk Manager, la persona que tiene la responsabilidad general de la administración del producto. Éstas son algunas de las tareas de las que se ocupa el administrador:

- Inicio y detención de los servicios necesarios para el servidor de CA Service Desk Manager.
- Configurar los diversos componentes del sistema.
- Determinar las opciones disponibles a los usuarios.
- Generar informes basados en los datos de Service Desk.

El objetivo de esta guía es ayudarlo a utilizar CA Service Desk Manager para implementar, gestionar e imponer la provisión de servicios. Esta guía lo ayuda a comprender cómo resuelve el producto el desafío de automatizar y gestionar por completo la provisión de servicios, desde que se producen los problemas hasta que se solucionan.

Información indispensable

Para administrar correctamente CA Service Desk Manager, deberá estar familiarizado con lo siguiente:

- El entorno operativo donde se instala CA Service Desk Manager
- La operación del servidor Web
- Tareas de administración básicas

Esta guía asume que el producto ha sido instalado correctamente, conforme a la información de la *Guía de implementación*.

Procesos y prácticas recomendadas para la gestión de los servicios

La aplicación de procesos normalizados y de las prácticas recomendadas ejerce una influencia directa en la eficacia, la productividad y el coste del entorno Service Support. CA ofrece una biblioteca de procesos y prácticas recomendados para la gestión de servicios que satisfaga los estándares del sector así como algunos marcos de mejores prácticas recomendadas que cuentan con amplio reconocimiento, como ITIL, CobIT o BS15000, entre otros. Los procesos para CA Service Desk Manager que se describen son los siguientes:

- Gestión de incidentes
- Gestión de problemas
- Gestión de cambios
- Gestión de solicitudes
- Gestión de la configuración
- Gestión de versiones
- Gestión del conocimiento
- Automatización de soporte

Nota: La información sobre la biblioteca de prácticas recomendadas está disponible en línea. Si desea conocer las prácticas recomendadas de CA en cuanto a la gestión de los servicios, que incluye las notas de los productos y otros documentos, visite <http://www.ca.com/sm/bp> <http://www.ca.com/sm/bp>. Los socios de CA, expertos en procesos estratégicos, pueden ser de ayuda para la personalización de la biblioteca de prácticas recomendadas en cada organización.

Capítulo 2: Gestión de servidores

Esta sección contiene los siguientes temas:

[Número de servidores](#) (en la página 27)
[Tareas de configuración del servidor](#) (en la página 28)
[Configuración de TCP/IP](#) (en la página 29)
[Cambio de la configuración de un servidor](#) (en la página 30)
[Configuración de ITIL](#) (en la página 30)
[Inicio de servidores secundarios](#) (en la página 37)
[Inicio del servidor principal](#) (en la página 38)
[Estado del servidor](#) (en la página 40)
[Configuración de SSL en Tomcat](#) (en la página 41)
[Cómo se implementan los servicios Web de CMDBf](#) (en la página 42)
[Cómo detener un servidor \(Windows\)](#) (en la página 43)
[Cómo detener un servidor \(UNIX\)](#) (en la página 43)

Número de servidores

La instalación de CA Service Desk Manager cuenta con al menos un componente de servidor que, en su calidad de administrador, debe gestionar. El número de servidores depende de la empresa. Cada instalación tiene un servidor primario que gestiona todas las funciones de CA Service Desk Manager. En ocasiones, las instalaciones tienen un servidor secundario o varios que gestionan funciones específicas. Después de haber instalado CA Service Desk Manager, es preciso configurar cada equipo en el que se ejecutan componentes del producto.

Por ejemplo, puede existir una configuración que conste de un solo equipo que haga de servidor principal en el que estén instalados todos los servicios necesarios. O bien, su instalación puede incluir varios equipos, cada uno de ellos realizando una función específica. Por ejemplo, un equipo puede actuar como servidor primario y servidor de bases de datos, mientras otro servidor Web distinto ejecuta la interfaz Web, y otro equipo más se encarga de autenticar los usuarios.

Puede ejecutar la configuración de servidor como parte del proceso de instalación, o puede ejecutarla más tarde. La configuración cambia si se producen cambios en su entorno.

Nota: Para obtener más información acerca de la arquitectura de este producto y las opciones de configuración, consulte la *Guía de implementación*.

Tareas de configuración del servidor

Se recomienda configurar cada equipo en el que se desee ejecutar CA Service Desk Manager. Como administrador, se debe configurar el servidor primario, el servidor secundario y las instalaciones de cliente. La configuración inicial se realiza como parte del proceso de instalación de CA Service Desk Manager.

En cualquier entorno de CA Service Desk Manager, se ejecutan las siguientes tareas:

- Configurar servidores
- Iniciar, detener y controlar el servidor primario
- Iniciar, detener y controlar un servidor secundario (si se define)

Nota: CA Service Desk Manager emplea el servidor de base de datos tanto para almacenar como para recuperar información. El servidor de base de datos se ejecuta como servicio separado. Para la información administrativa, refiérase a la documentación del servidor de base de datos.

Un cambio en el entorno del sistema puede requerir cambios en la configuración del servidor. Por ejemplo, se puede cambiar la configuración del servidor de CA Service Desk Manager debido a las siguientes razones:

- Cambios en el sistema de gestión de bases de datos
- Cambios hechos al archivo de la plantilla de inicio de CA Service Desk Manager por `pdm_edit.pl` (una opción usada para agregar funcionalidad y aumentar el rendimiento del sistema empresarial)
- Integración con un servidor Web como Tomcat
- Integración con CA EEM

Configuración de TCP/IP

Puede cambiar la configuración del protocolo de Internet de TCP (TCP/IP) predeterminado en uno o más servidores. Esta configuración no se puede imponer en el cliente si no es compatible con el servidor.

La configuración de TCP/IP se controla mediante el archivo `NX.env`, que se encuentra en el directorio `$NX_ROOT`. Utilice un editor de texto como WordPad para editar este archivo. La siguiente opción controla la configuración del TCP/IP:

```
NX_PROTOCOL_ONLY=modo
```

donde *modo* puede ser uno de los siguientes valores:

IPv4

En el modo IPv4, el sistema abre sockets para procesos slump que escuchan el tráfico de IPv4.

IPv6

En el modo IPv6, el sistema abre sockets para procesos slump que escuchan el tráfico de IPv6.

Mixto

En el modo mixto, el sistema abre sockets para procesos slump que escuchan el tráfico de IPv4 e IPv6. El modo mixto está diseñado para clientes con servidores secundarios que utilizan un Protocolo de Internet diferente del servidor primario (o el uno al otro).

Nota: Si los hosts de IPv4 y de IPv6 coexisten en la red, asegúrese de que las estrategias de transición, las herramientas y los mecanismos apropiados para respaldar estas tecnologías estén en su lugar antes de que cambie la configuración del servidor.

Ejemplo

```
NX_PROTOCOL_ONLY=ipv4
```

Cambio de la configuración de un servidor

Puede usar la función de configuración para hacer cambios en la configuración de un servidor.

Procedimiento para cambiar la configuración de un servidor

1. En el menú Inicio de Windows, seleccione Programas, CA, CA Service Desk Manager, Configuración.

Aparece la utilidad Configuración de CA Service Desk Manager.

2. Rellene los campos de la utilidad y haga clic en Siguiente.

El panel derecho cambia para mostrar los campos pertinentes para el vínculo resaltado en el panel de navegación de la izquierda.

3. Continúe siguiendo las instrucciones que van apareciendo en pantalla para realizar la instalación y luego haga clic en Finalizar.

La configuración del servidor queda cambiada.

Configuración de ITIL

La *Biblioteca de infraestructura de tecnologías de la información (ITIL)* es una recopilación de prácticas recomendadas en la gestión de centros de datos informáticos. Además de definir los procesos recomendados, una ventaja principal del marco de ITIL es su estrecha definición de la terminología de los centros de datos comúnmente utilizada. Con frecuencia, en el mundo de la TI se utiliza la misma palabra para hacer referencia a cosas diferentes; o cada persona utiliza una palabra determinada con un matiz individual. ITIL contribuye a evitar este tipo de problema.

Se encuentran disponibles los siguientes tipos de tickets:

- Solicitud
- Orden de cambios
- Incidencia
- Incidente
- Problema

Importante: CA Service Desk Manager solamente admite una interfaz ITIL.

La interfaz ITIL admite objetos de datos que no fueron usados en versiones anteriores del producto que no eran ITIL; por ejemplo, tickets de problema y de incidente.

ITIL realiza lo siguiente:

- Produce una interfaz ITIL para la instalación de CA Service Desk Manager.
- Permite que la base de datos, los formularios y los campos de CA Service Desk Manager difieran de una instalación estándar, por lo que se adaptan a convenciones de ITIL.

Importante: Al actualizar el sistema existente, es necesario desactivar la casilla de verificación si desea conservar los datos y las tablas de las bases de datos; de lo contrario, todos los datos existentes se perderán.

Disciplinas del servicio de ITIL

ITIL describe las prácticas recomendadas para varias disciplinas. Las disciplinas de Service Support y Service Delivery se combinan para proporcionar la capacidad de gestión de servicios a una organización. Las interrelaciones complejas entre las diez disciplinas de la gestión de servicios interactúan para ayudar a garantizar que la infraestructura de TI entregue a las empresas un nivel de servicio alto.

El soporte de servicio incluye las siguientes disciplinas:

- Gestión de incidentes
- Gestión de problemas
- Gestión de cambios
- Gestión de versiones
- Gestión de la configuración

CA Service Desk Manager aborda específicamente la gestión de incidentes, problemas, cambios y configuración.

La provisión de servicios incluye las siguientes disciplinas:

- Service Management
- Gestión de disponibilidad
- Gestión de capacidad
- Gestión financiera para servicios de TI
- Gestión de continuidad de los servicios de TI

CA Service Desk Manager específicamente aborda la gestión de servicios.

Opciones de la interfaz de empleados y de invitados

Puede utilizar CA Service Desk Manager para configurar interfaces separadas para empleados e invitados. Configure estas interfaces separadas a través del Gestor de opciones en la ficha Administración. Los siguientes valores controlan estas interfaces:

employee_intf_incident_support

Muestra los siguientes valores:

- Sólo solicitudes
- Incidente sólo
- Incidentes y solicitudes

guest_intf_incident_support

Muestra los siguientes valores:

- Sólo solicitudes
- Incidente sólo
- Incidentes y solicitudes

Importante: Si es una nueva instalación, se configura ITIL de forma predeterminada con el valor establecido en *Sólo incidente*. Si está migrando de una configuración anterior que no es de ITIL, se instalan las opciones, pero los valores se establecen a *Sólo solicitudes*.

Configuración de la interfaz de empleados

Puede configurar la interfaz de empleados para mostrar incidentes, solicitudes o ambos.

Procedimiento para configurar la interfaz de empleados

1. Haga clic en la ficha Administración.
Aparecerá la consola de administración.
2. Haga clic en Gestor de opciones, Gestor de solicitudes.
Aparecerá la lista de opciones.
3. Haga clic en employee_intf_incident_support.
Aparecerá la página Detalles de opciones.
4. Cambie el campo Valor de opción por uno de los siguientes valores:

Sólo incidente

(ITIL predeterminado) Muestra solamente los tipos de ticket de incidente en la interfaz de empleados.

Sólo solicitudes

Muestra solamente los tipos de ticket de solicitud en la interfaz de empleados.

Incidentes y solicitudes

Muestras tanto los tipos de ticket de incidente como de solicitud en la interfaz de empleados.

Haga clic en Guardar.

5. Haga clic en Actualizar para confirmar las selecciones.

Se actualiza el Detalle de opciones.

6. Cierre el Detalle de opciones.

Aparecerá la lista de opciones.

Configuración de la interfaz de invitados

Puede configurar la interfaz de invitados para mostrar incidentes, solicitudes o ambos.

Procedimiento para configurar la interfaz de invitados

1. Haga clic en la ficha Administración.

Aparecerá la consola de administración.

2. Haga clic en Gestor de opciones, Gestor de solicitudes.

Aparecerá la lista de opciones.

3. Haga clic en `guest_intf_incident_support`.

Aparecerá la página Detalles de opciones.

4. Cambie el campo Valor de opción por uno de los siguientes valores:

Sólo incidente

(Predeterminado) muestra solamente los tipos de ticket de incidente en la interfaz de invitados.

Sólo solicitudes

Muestra solamente los tipos de ticket de solicitud en la interfaz de invitados.

Incidentes y solicitudes

Muestras tanto los tipos de ticket de incidente como de solicitud en la interfaz de invitados.

Haga clic en Guardar.

5. Haga clic en Actualizar para confirmar las selecciones.
Se actualiza el Detalle de opciones.
6. Cierre el Detalle de opciones.
Aparecerá la lista de opciones.

Notificaciones de elementos de configuración

Un elemento de configuración le permite definir una notificación de actividades que se asocia con un elemento de configuración específico que, a su vez, se asocia con un ticket de CA Service Desk Manager específico. Esta función le permite seguir información sobre los usuarios, las organizaciones y los distribuidores de un elemento de configuración.

Puede especificar los contactos de objeto de CI en la página Receptores de actualización de reglas de notificación, como CI Org mant, CI Contacto primario y así sucesivamente.

Seguridad del registro de actividades

La opción de seguridad del registro de actividades impide que los usuarios finales actualicen los campos de un registro de actividades. Puede seleccionar la opción Interno para evitar que un cliente consulte el registro.

La seguridad del registro de actividades afecta los registros de actividades de los tipos de ticket siguientes:

- Solicitud
- Orden de cambio
- Incidencia
- Incidente
- Problema

Cómo habilitar la seguridad del registro de actividades

Puede habilitar la seguridad del registro de actividades desde el Gestor de opciones en la ficha Administración.

Procedimiento para habilitar la seguridad del registro de actividades

1. Haga clic en la ficha Administración.
Aparecerá la consola de administración.

2. Haga clic en Gestor de opciones, Solicitud-cambio-incidencia.
Aparecerá la lista de opciones.
3. Haga clic en activity_log_security.
Aparecerá la página Detalles de opciones.
4. Haga clic en Editar y seleccione uno de los siguientes valores de opción:

Editable

(Predeterminado) Permite que todos los campos del registro de actividades sean editables a través de la interfaz Web o los servicios Web.

Protegido contra escritura

Muestra el registro de actividades como de sólo lectura. Si selecciona la opción interna, sólo los usuarios internos pueden editar el registro y no puede ser visto por el cliente.

Nota: Si la opción de seguridad está habilitada, aparece un mensaje de error acerca de que el registro de actividades es de sólo lectura si se intenta editar el registro a través de la interfaz Web o fuentes externas como servicios Web.

Haga clic en Guardar.

5. Haga clic en Actualizar para confirmar las selecciones. Cierre la ventana.
Se habilita la seguridad del registro de actividades.

Importante: la opción activity_log_security no se puede desinstalar. Puede cambiar solamente el valor de la opción a Editable o Protegido contra escritura en el Gestor de opciones, Solicitud-cambio-incidencia.

Impacto en Web Screen Painter

La función de seguridad del registro de actividades, \$NX_ACTIVITY_LOG_SECURITY, incluye los siguientes atributos (time_spent, time_stamp y descripción) de los objetos alg, chgalg, issalg en majic.

Ejemplo: \$NX_ACTIVITY_LOG_SECURITY para alg de objeto en cm.maj

En este ejemplo, para alg de objeto en cm.maj, \$NX_ACTIVITY_LOG_SECURITY aparece en los tres atributos:

```
time_spent DURATION $NX_ACTIVITY_LOG_SECURITY {ON_POST_VAL update_cr_timespent(
call_req_id ) 50 ;
} ;
time_stamp DATE $NX_ACTIVITY_LOG_SECURITY { ON_NEW DEFAULT NOW ; } ;
description STRING $NX_ACTIVITY_LOG_SECURITY;
```

En Web Screen Painter, el campo *Actualizable sólo para registro nuevo* queda desactivado cuando el valor de la palabra clave se evalúa como WRITE_NEW.

Nota: Para obtener información sobre Web Screen Painter, consulte la *Guía de implementación*.

Interfaz PDA

CA Service Desk Manager admite la terminología de ITIL para interfaces de agendas electrónicas (PDA). En la interfaz para PDA se muestran los siguientes tipos de ticket:

- Incidentes
- Problemas
- Solicitudes
- Solicitudes de cambio
- Incidencias

Para deshabilitar la interfaz de PDA, sólo tiene que comentar la línea *PDAHtmlPath* del archivo de configuración. Si está deshabilitada, los usuarios ven la interfaz de los analistas o los clientes, según corresponda.

Sólo se aceptan las solicitudes de acceso a interfaces de PDA en el caso de los usuarios analistas. Cuando se conecta a la interfaz de PDA, su rol se establece en el rol que estaba utilizando cuando inició sesión por última vez fuera de la interfaz de analista Web de CA Service Desk Manager.

Cualquier usuario que típicamente inicie sesión en la interfaz de analista Web de CA Service Desk Manager puede solicitar que la interfaz de PDA se conecte introduciendo su *ID de usuario* en la página de inicio de sesión con pda del siguiente modo:

`pda:userid`

Por ejemplo, puede acceder a la interfaz de PDA de un dispositivo que no sea PDA, como un equipo de escritorio o portátil proporcionando las credenciales de **pda:userid** y de contraseña.

Inicio de servidores secundarios

Si la instalación incluye uno o más servidores secundarios, debe iniciar los servidores secundarios antes de iniciar el servidor primario.

En el entorno UNIX, cada servidor secundario de CA Service Desk Manager se inicia en la línea de comandos mediante `pdm_proctor_init`.

En un entorno Windows, cada servidor secundario de CA Service Desk Manager se inicia mediante el servidor del supervisor remoto.

Procedimiento para iniciar un servidor secundario en Windows

1. Seleccione Servicios en el panel de control.
Aparece el Panel de control.
2. Seleccione el servicio del supervisor remoto de CA Service Desk Manager y haga clic en Inicio.
El servicio se ha iniciado.

Más información:

[pdm_proctor_init: inicio del supervisor en servidores secundarios](#) (en la página 1037)

Inicio del servidor principal

Todas las instalaciones de CA Service Desk Manager disponen de un servidor primario que se encarga de las funciones básicas del producto.

Importante: Si la instalación incluye uno o más servidores secundarios, debe iniciar los servidores secundarios antes de iniciar el servidor primario.

Para iniciar el servidor primario de CA Service Desk Manager en un entorno de Windows, en el Panel de control, seleccione el servicio del servidor de CA Service Desk Manager y haga clic en Iniciar. Se puede iniciar el servicio manualmente cada vez que sea necesario o configurarlo para que se inicie de forma automática al igual que cualquier otro servicio de Windows.

En el entorno UNIX, el servidor de CA Service Desk Manager se inicia desde la línea de comandos mediante `pdm_init`.

La siguiente tabla describe los procesos que se inician automáticamente cuando inicia el servidor de CA Service Desk Manager:

Proceso	Descripción
Daemon Agent (<code>pdm_proctor_nxd</code>)	Es el agente de daemons responsable de iniciar los daemons gestionados.
Control de daemons (<code>pdm_d_mgr</code>)	Controla los procesos de daemons.
Base de datos virtual de BOP (<code>bpvirtdb_srvr</code>)	Servidor de base de datos virtual de BOP
Data Dictionary (<code>ddictbuild</code>)	Regenera el diccionario de datos cada vez que se inicia el sistema; se ejecuta y, después, desaparece.
KPI Daemon (<code>kpi_daemon</code>)	Gestiona la recopilación, la organización y el almacenamiento de los datos del KPI.
Agente de Oracle (<code>orcl_agent</code>)	Agente de la base de datos Oracle; tiene muchas instancias en función de la carga.
Oracle DB (<code>orcl_prov_nxd</code>)	Proveedor de base de datos de Oracle
SQL agent (<code>sql_agent</code>) (sólo se ejecuta si se utiliza MS SQL)	Agente para la base de datos de SQL Server; muchas instancias, dependiendo de la carga
SQL DB (<code>sql_prov_nxd</code>) (sólo se ejecuta si se utiliza MS SQL)	Proveedor de la base de datos Microsoft SQL Server
Event Manager (<code>ehm_nxd</code>)	Gestor de eventos

Proceso	Descripción
License Manager (license_nxd)	Gestiona la seguridad
Distribuidor de mensajes (sslump_nxd)	Distribuye los mensajes
Notification Manager (sólo Windows) (bpnotify_nxd)	Gestiona las notificaciones en el entorno Windows
Object Engine (domsrvr)	Servidor de CA Service Desk Manager
Report Manager (pcrpt_nxd)	Generación de informes de equipos
Software Version Control (pdm_ver_nxd)	Gestiona las versiones de los componentes del sistema especificados
Method Engine (spel_svr)	Servidor que interpreta el código ortográfico
Text API (pdm_text_nxd)	Daemon de TextAPI para correo electrónico e interfaces de CA NSM
Timed Events/Notifications (animator_nxd)	Eventos y notificaciones temporizados
User Validation (boplgln)	Inicio de sesión para la gestión de solicitudes
Web Engine (webengine)	Ejecuta el motor del servicio Web
Archive Purge Daemon (arcpur_svr)	Gestiona el procesamiento en segundo plano de almacenamiento y depuración
BU Daemon (bu_daemon)	Se ocupa de calcular la clasificación de preguntas frecuentes de los documentos de conocimiento
DB Monitor (dbmonitor_nxd)	Controla las tablas comunes de CA en busca de cambios
EBR Daemon (bpebr_nxd)	Se ocupa de las solicitudes de búsqueda de conocimientos
EBR Idx Daemon (bpeid_nxd)	Se ocupa de reindexar EBR
Multi-site SD Daemon (global_nxd)	Gestiona la réplica en segundo plano para el procesamiento en varios sitios
KRC Daemon (krc_daemon)	Gestiona el cálculo estadístico y las notificaciones de la tarjeta de informes de conocimiento
KT Daemon (kt_daemon)	Gestiona los documentos de conocimiento (proceso de aprobación de documentos de conocimiento, permisos, notificaciones, etc.)

Proceso	Descripción
LDAP virtddb (ldap_virtddb)	Agente para la comunicación con los servidores LDAP
Mail Daemon (pdm_mail_nxd)	Gestiona las notificaciones por correo electrónico salientes
Mail Eater (pdm_maileater_nxd)	Gestiona las notificaciones por correo electrónico entrantes
MDB Registration Server (mdb_registration_nxd)	Agente que se encarga de gestionar las solicitudes de registro de MDB
PDM KTLC (pdm_ktlc)	Gestiona las licencias de Gestión del conocimiento.
PDM RPC (PDM_RPC)	Gestiona las solicitudes de servicios Web
Repository Daemon (rep_daemon)	Se ocupa de los repositorios de archivos adjuntos
Spell checker (lexagent_nxd)	Se ocupa de las solicitudes de revisión ortográfica
Time-to-Violation (ttv_nxd)	Indica el pronosticador de infracciones del acuerdo de nivel de servicio.
tomcat controller (pdm_tomcat_nxd)	Gestiona los servicios Tomcat

Nota: En la tabla anterior, el proceso Notification Manager es aplicable sólo al entorno Windows y, el proceso Default DB, al entorno de UNIX.

Estado del servidor

Puede usar la utilidad pdm_status para mostrar el estado de los servidores primario o secundario de CA Service Desk Manager que se ejecuten en cualquier entorno operativo.

Configuración de SSL en Tomcat

Puede configurar su sistema para utilizar Secure Socket Layer (SSL) en un servidor Web de Tomcat.

Procedimiento para configurar SSL con Tomcat

1. En la línea de comandos, cambie el directorio a la ubicación de instalación de JRE e introduzca este comando:

```
bin\keytool -genkey -alias tomcat -keyalg RSA
```

Un archivo .keystore se crea de forma predeterminada en el directorio principal del usuario inició sesión. No obstante, es posible especificar otra ubicación durante la generación del archivo .keystore. En UNIX, es necesario asegurarse de que el directorio en el que se genere el archivo .keystore disponga de permisos suficientes para acceder a CA Service Desk Manager.

Nota: Para obtener más información acerca de la especificación de una ubicación diferente para el archivo .keystore, consulte la documentación de Tomcat.

2. Conteste de forma adecuada a los mensajes que aparecen en la pantalla. La contraseña predeterminada es *changeit*.

Nota: Puede introducir una contraseña que no sea la predeterminada. Para obtener más información, consulte la documentación de Tomcat.

3. Edite el archivo *server.xml* ubicado en el siguiente directorio:

```
NX_ROOT\bopcfg\www\CATALINA_BASE\conf.
```

4. Anule los comentarios de la sección de SSL y agregue la ubicación del archivo .keystore generado en el Paso 1:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8443" minProcessors="5" maxProcessors="75"
enableLookups="true"
acceptCount="100" debug="0" scheme="https" secure="true"
useURValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
clientAuth="false" protocol="TLS" keystoreFile="C:\Documents and
Settings\user\.keystore" />
</Connector>
```

5. Utilice los siguientes comandos para reiniciar el servidor de Tomcat:

```
pdm_tomcat_nxd -c stop
pdm_tomcat_nxd -c start
```

6. Para tener acceso a la interfaz Web de CA Service Desk Manager con SSL, utilice `https://nombre_equipo:8443/CAisd/pdmweb.exe`. También puede derivar la dirección URL de los servicios Web de un modo similar.

Nota: Si lo desea, especifique un puerto que no sea el 8443 en el archivo `server.xml`.

7. Consulte e instale el certificado SSL necesario para acceder a CA Service Desk Manager.

El sistema se configura para utilizar Secure Socket Layer (SSL) en un servidor Web de Tomcat.

8. (Opcional) Si está teniendo acceso a CA Service Desk Manager con Internet Explorer y Windows Server 2003 está configurado para SSL, el explorador requiere que se realice configuración adicional y se reinicie. En Opciones de Internet, en la ficha Opciones avanzadas, desactive las siguientes opciones en la sección Seguridad:

- Comprobar la revocación de certificados del servidor (requiere reiniciar)
- No guardar las páginas cifradas en el disco

Después de reiniciar el explorador, podrá tener acceso a CA Service Desk Manager a través del servidor Tomcat basado en SSL.

Cómo se implementan los servicios Web de CMDBf

Después de que se instale CA Service Desk Manager, puede implementar servicios Web de CMDBf.

Para implementar los servicios Web de CA CMDB

1. Asegúrese de que el servidor Web está en funcionamiento.
2. Desplácese al directorio `CMDBHOME\sdk\websvc\CMDBF`.
3. Ejecute `deploy_cmdbws.bat`.

Se implementan y se inician los servicios Web de CMDBf.

Cómo detener un servidor (Windows)

Puede detener un servidor de CA Service Desk Manager primario o secundario en un entorno Windows.

Procedimiento para detener un servidor de CA Service Desk Manager en un entorno Windows

1. Seleccione Servicios en el panel de control.
Se abrirá la ventana Servicios.
2. Seleccione el servicio que quiere detener haga clic en Detener:

Servidor de CA Service Desk Manager

Controla el servidor primario.

Supervisor remoto de CA Service Desk Manager

Controla un servidor secundario.

El servidor se detiene.

Cómo detener un servidor (UNIX)

Puede detener un servidor de CA Service Desk Manager primario o secundario en un entorno UNIX.

Procedimiento para detener un servidor de CA Service Desk Manager en un entorno UNIX

1. Cierre todos los clientes de CA Service Desk Manager.
2. Detenga el servidor; para ello, ejecute la utilidad `pdm_halt`.
El servidor se detiene.

Más información:

[pdm_halt: finalización de demonios o detención de servicios](#) (en la página 1023)

Capítulo 3: Definición de la estructura empresarial

Esta sección contiene los siguientes temas:

[Cómo definir la estructura de negocio](#) (en la página 45)

[Definición de la infraestructura empresarial](#) (en la página 48)

[Asistencia multidepartamental](#) (en la página 52)

[Multicliente](#) (en la página 67)

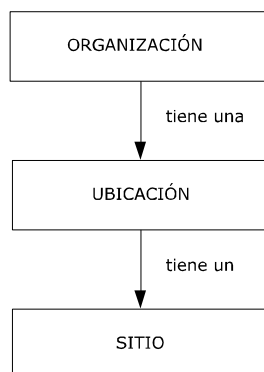
Cómo definir la estructura de negocio

La *estructura de negocio* es una representación lógica de la organización en la que opera CA Service Desk Manager. Para personalizar la instalación, puede configurar los objetos de la estructura de negocio para que se adapte mejor a sus necesidades.

Se configuran los objetos siguientes para definir la estructura de negocio:

- Departamentos
- Ubicaciones
- Organizaciones

El diagrama siguiente ilustra la relación entre los objetos de la estructura de negocio:



Porque una organización tiene una ubicación (o referencias a ella), que a su vez tiene un sitio, debe definir los objetos en la siguiente secuencia:

1. Departamentos
2. Ubicaciones
3. Organizaciones

De este modo, al definir cada objeto, cabe la posibilidad de elegir uno de los objetos existentes en los niveles inferiores de la jerarquía.

Nota: Si desea obtener más información sobre la definición de cada objeto, consulte la *ayuda en línea*.

Contactos

Puede definir a cada persona que utilice su sistema con regularidad, como por ejemplo analistas y clientes. Estas personas se denominan contactos.

Grupos

Los grupos son recopilaciones de contactos que representan áreas específicas de responsabilidad dentro del servicio de asistencia. Al definir grupos, se puede asignar la responsabilidad de la resolución de partes concretas cuando dicha responsabilidad la comparten varios individuos.

Por ejemplo, supongamos que tenemos un grupo que corresponde al sitio de recursos humanos de Zaragoza, el cual es responsable de solucionar los problemas del personal de la oficina que tiene la organización en esta ciudad. Cada vez que un empleado de esa oficina tiene algún problema, se le puede asignar al grupo anterior para su resolución.

A los grupos se les pueden asociar áreas de solicitud, ubicaciones o turnos y emplearlos para determinar cuándo estarán los contactos del grupo disponibles para la asignación automática de solicitudes.

Departamentos

Los *sitios* son agrupaciones de ubicaciones. Se entiende por departamento, por ejemplo, una ciudad en la que la empresa cuenta con una o varias ubicaciones físicas, o una región en la que hay presente una clientela a la que se proporciona asistencia. Como las ubicaciones hacen referencia a los departamentos, éstos se deben definir antes que las primeras. Esta secuencia permite utilizar el sitio nuevo en la ubicación.

Ubicaciones

Ubicaciones identifica un lugar físico específico y le permite seguir y administrar áreas que conciernen a su empresa, como la dirección de una compañía en particular, una ciudad de dirección de oficina, un campus, un edificio o incluso un piso de un edificio.

Las ubicaciones son los únicos objetos a los que es posible asociar direcciones físicas; los demás objetos (organizaciones, elementos de configuración y contactos, por ejemplo) derivan sus respectivas direcciones de las ubicaciones asociadas.

Debería definir ubicaciones antes de las organizaciones; esta secuencia le permite utilizar la ubicación nueva en la organización.

Puede utilizar ubicaciones para asignar solicitudes automáticamente. Para activar la asignación automática en función de la ubicación, asigne las ubicaciones a las áreas de solicitud y los grupos. Las ubicaciones pertenecientes a las áreas de solicitud se utilizan para coincidir cada solicitud con una ubicación según la ubicación del usuario final afectado o el elemento de configuración de la solicitud. Las ubicaciones pertenecientes a los grupos se emplean, a continuación, para seleccionar un grupo apto para la asignación automática de solicitudes de la ubicación en cuestión.

Nota: En la ficha Administración, se hace referencia a los tickets como áreas de solicitud/incidente/problema. Para abreviar, aquí se denominan áreas de solicitud.

Organizaciones

Las *organizaciones* describen divisiones y departamentos internos o compañías externas que se pueden asignar a tickets, clases de elementos de configuración y contactos (por ejemplo, se utilizan para identificar las empresas a las que están asociados los clientes).

Existe la opción de asignar tipos de servicios predeterminados a las organizaciones, los cuales se asignan automáticamente a los tickets si se especifica la organización. Esto permite asociar un nivel de servicio específico a los tickets según la organización asignada.

Puede definir los elementos de configuración para las organizaciones, lo que permite especificar el hardware, el software y los servicios que éstas emplean. La vinculación de elementos de configuración a una organización (elementos de configuración compartidos) complementa la función de vinculación directa de elementos de configuración a los contactos (elementos de configuración privados). Al designar un contacto como usuario final afectado de una solicitud, se puede seleccionar un elemento de configuración para la solicitud en las listas independientes de elementos de configuración compartidos y privados.

Definición de la infraestructura empresarial

Un aspecto importante de la implementación de centro de servicio al usuario con CA Service Desk Manager radica en la definición de la infraestructura empresarial mediante la configuración de lo siguiente:

- Clases y familias de elementos de configuración
- Fabricantes y modelos
- Estados de servicio
- Distribuidores y tipos de distribuidores

La información siguiente proporciona una descripción general para cada objeto y explica cómo el objeto se utiliza en el producto.

Nota: Si desea obtener más información sobre la definición de cada objeto, consulte la *ayuda en línea*.

Orden de definición de objetos

Cuando se definen objetos, se empieza por los niveles inferiores de la jerarquía de objetos. De este modo, cuando se definen objetos en niveles más altos, puede seleccionar entre los objetos existentes en los niveles inferiores de la jerarquía. Por ejemplo, como una clase tiene (referencias) una familia, primero se define las familias y luego las clases. De forma similar, como los elementos de configuración se encuentran en lo más alto de la jerarquía, es necesario definirlos en último lugar, después de definir todos los objetos que los sustentan. Por tanto, los objetos de datos se definen en el orden siguiente:

Definir Primero	Definir Segundo	Definir Tercero
Familias	Clases	Elementos de configuración
Fabricantes	Modelos	Elementos de configuración
Estados de servicio	Elementos de configuración	

Definir Primero	Definir Segundo	Definir Tercero
Tipos de distribuidores	Distribuidores	Elementos de configuración

Familias y clases

Las *familias* clasifican los elementos de configuración por tipo y asignan atributos significativos a cada uno de ellos. Las *clases* permiten identificar las categorías generales de los elementos de configuración que admite la empresa. Las familias son categorías amplias de elementos de configuración, por ejemplo, el hardware, el software y los servicios. Las clases, en cambio, son categorías más específicas dentro de las categorías más amplias que constituyen las familias. Por ejemplo, la familia de hardware puede contener clases como módems, enrutadores, repetidores o puentes.

La organización de los elementos de configuración en familias y clases facilita su gestión. Por ejemplo, se podría generar una lista de elementos de configuración que pertenezcan a una familia o clase determinada.

Fabricantes y modelos

Los *fabricantes* permiten identificar los fabricantes de los diversos elementos de configuración que interesan a la empresa. Los *modelos* contienen información específica sobre los productos que cada fabricante suministra a la empresa. Así, si se define como fabricante a una determinada compañía de software, se definirían como modelos cada una de las aplicaciones que dicha compañía suministra a la empresa.

La definición de fabricantes y modelos facilita la gestión de los elementos de configuración. Por ejemplo, se podría generar una lista de los modelos que suministra un determinado fabricante y otra de los elementos de configuración de cada modelo concreto.

Estado de servicio

Los *estados de servicio* identifican el estado de operatividad de los elementos de configuración. Como ejemplos de estados de servicio se incluyen: *en servicio*, *en reparación* o *interrumpido*. La definición de estados de servicio facilita el seguimiento de la disponibilidad y el uso de los elementos de configuración de la empresa. Para ello, por ejemplo, se podría elaborar una lista de elementos de configuración que se encuentren actualmente en reparación.

Distribuidores y tipos de distribuidores

Los *tipos de distribuidores* son clasificaciones de los distribuidores que permiten identificar el tipo de compañía que suministra los elementos de configuración. Así, por ejemplo, se podría clasificar a los distribuidores a los que se arrienden elementos de configuración como arrendadores y, a los que presten un servicio a la empresa, como proveedores.

Los *distribuidores* permiten identificar a las compañías que proveen a la empresa, con inclusión del tipo de compañía y un contacto principal. Además de hacer referencia a los distribuidores en los elementos de configuración, también se puede hacer en los registros de contactos de los usuarios.

La definición de distribuidores y tipos de distribuidores es una manera cómoda de organizar los elementos de configuración. Para ello, por ejemplo, se podría elaborar una lista de los distribuidores que encajan en un determinado tipo de distribuidor y otra de los elementos de configuración de cada distribuidor.

Elementos de configuración

Los *elementos de configuración* son los dispositivos, el software y los servicios que componen la infraestructura empresarial. La información asociada con un elemento de configuración identifica unívocamente el elemento de configuración e indica su ubicación concreta. Los elementos de configuración se pueden asociar con contactos (elementos de configuración privados) y organizaciones (elementos de configuración compartidos). Los elementos de configuración permiten identificar, ver y especificar lo siguiente:

- Identificar elementos de configuración por nombre, clase y familia.
- Especificar información sobre el inventario.
- Especificar otras propiedades que definen los elementos de configuración.
- Registrar y ver comentarios asociados a los elementos de configuración.
- Especificar información de ubicación para los elementos de configuración.
- Especificar información de servicio (como el tipo de servicio) para los elementos de configuración.
- Ver y definir los contactos y organizaciones asignados a los elementos de configuración.

- Identificar relaciones jerárquicas y de punto a punto entre elementos de configuración.
- Ver los partes asociados a los elementos de configuración.

No es obligatorio definir toda esta información para los elementos de configuración. Sin embargo, si define una cantidad óptima de información sobre los elementos de configuración obtendrá una imagen más clara cuando se realice el análisis del impacto para la organización de TI.

Herramientas externas de gestión de activos

Puede integrar la instalación de CA Service Desk Manager con otras herramientas de gestión de activos como CA NSM, Asset Management de CA y CA APM. Las funciones de gestión de activos de estas herramientas de CA Service Desk Manager incluyen lo siguiente:

- CA NSM proporciona la utilidad de pdm_nsmimp (para Windows solamente) para agregar información de activos a CA Service Desk Manager.
- Asset Management de CA proporciona un conjunto completo de hardware y funciones del inventario de software. Al ver un elemento de configuración en el cliente de CA Service Desk Manager, puede hacer clic en el botón Visor de activos para ver más información que se haya descubierto sobre el activo.

La integración entre CA Service Desk Manager y CA Asset Management se activa cuando se instalan ambos productos en la misma MDB.

- Unicenter Asset Portfolio Management proporciona un conjunto completo de funciones de ciclo de vida del activo. Al ver un elemento de configuración en el cliente de CA Service Desk Manager, puede hacer clic en el botón Visor de activos para ver más información financiera sobre el activo.

La integración entre CA Service Desk Manager y Unicenter Asset Portfolio Management se activa cuando se instalan ambos productos en la misma MDB.

Nota: Para obtener más información sobre la integración de su instalación de CA Service Desk Manager con otras herramientas de gestión de activos, consulte la *Guía de implementación*.

Asistencia multidepartamental

Es posible configurar el acceso global de CA Service Desk Manager de manera que varias instalaciones de CA Service Desk Manager puedan compartir los datos. Consideremos las situaciones siguientes:

- Los centros de servicio al usuario globales requieren varias instalaciones regionales de CA Service Desk Manager que comparten o no la misma versión de CA Service Desk Manager o el mismo grado de personalización. Estas instalaciones regionales suelen estar ubicadas alrededor del mundo y los analistas de una región ofrecen asistencia fuera del horario normal a los clientes con sede en otra. Esto se llama también atención ininterrumpida o permanente. Los analistas tienen que ser capaces de prestar su servicio a los clientes donde estén ubicados.
- Las instalaciones regionales múltiples de CA Service Desk Manager disponen de grupos de analistas que deben trabajar en las colas de más de una instalación regional. Así, los analistas de un grupo especializado deben ver las colas de un grupo determinado en todas las instalaciones.

En ambos casos, existe la necesidad de mantener reglas de negocio que, en ocasiones, son contradictorias según la instalación. La asistencia multidepartamental permite salvar la distancia entre estas instalaciones separadas (denominadas regiones) a la vez que se mantienen reglas de negocio independientes para cada región.

Los analistas del servicio técnico que gestionan llamadas globales tienen la posibilidad de buscar contactos en todas las regiones así como de abrir partes o acceder a ellos desde una única ventana. Una vez creados los tickets, se transfiere a los analistas a la región apropiada (local o remota), donde se aplican las reglas de negocio pertinentes.

Además, los analistas que gestionan partes de varias regiones también pueden ver una lista de todos sus partes en una sola ventana. Al acceder a los detalles de un determinado ticket, los analistas se transfieren a la región apropiada (local o remota), donde se aplican las reglas de negocio pertinentes.

Descripción general del soporte de varios sitios

El servicio de soporte de varios sitios permite disponer de soporte global (distribuido). Puede admitir usuarios locales mediante servidores locales, pero permitir acceso a su servidor desde cualquier ubicación.

El soporte de varios sitios permite:

- La gestión de llamadas fuera del horario laboral a través de varias regiones.
- El soporte de expertos globales en varias regiones .
- Apagar el servidor primario de CA Service Desk Manager durante ventanas de mantenimiento sin afectar al resto de los elementos de la arquitectura de varios sitios.

Acciones de varios sitios

- Impone reglas de negocio regionales
- Permite abrir y revisar tickets
- Permite que los analistas globales trabajen en colas a través de varias regiones
- Reproduce datos mínimos
- Permite que las regiones estén en niveles de mantenimiento diferentes
- Permite que las regiones utilicen diferentes versiones de idioma

Importante: La página del código de equipo debe ser idéntica en todos los servidores primarios para evitar que los datos resulten dañados.

Acciones no de varios sitios

- No transfiere tickets entre regiones
Los tickets de soporte permanecen en el sitio en el que se crearon.
- No permite una generación de informes globales
Se puede generar informes de forma limitada en tablas Cola global.
- No permite la edición de datos replicados, como documentos de conocimiento.
Estos datos son de sólo lectura.

Información indispensable

Si desea utilizar el soporte de varios sitios, tenga en cuenta la información siguiente:

- Al cambiar la dirección IP de una región que participa, realice una de las siguientes acciones:
 - Recicle la región de Service Desk
 - Desactive y luego vuelva a activar el registro Región global para esa región.

- Los analistas globales deben tener la misma ID de inicio de sesión en todas las regiones.
- Las zonas de servidor y alias le permiten tener analistas globales que se ocupan de problemas como Internet, Intranet, DMZ, etc.
- Puede personalizar datos replicados.
Nota: Esta personalización puede exigir la modificación del archivo `global_sd.xml` en `$NX_ROOT/site/cfg`.
Importante: pruebe su archivo `global_sd.xml` modificado utilizando `pdm_global_nxd -x`.
- Los datos de elementos de configuración no son replicados.
- No se replican documentos de conocimiento.
- Debe actualizar los Ir a Recursos de un rol al realizar la implementación de varios sitios.

Importante: las configuraciones de varios sitios son diferentes a las instalaciones multicliente. Para obtener más información sobre la capacidad multicliente, vea Multicliente (see page 67).

Configuración de un sistema CA Service Desk Manager de varios sitios

Puede configurar un sistema de varios sitios desde el Gestor de opciones de la ficha Administración.

Procedimiento para configurar un sistema de varios sitios

1. En primer lugar, decida la instalación que va a ser la región master.
2. (Todas las regiones) Configure e instale la opción `global_name` desde Gestor de opciones, Varios sitios.
3. Recicle los servicios.

Importante: El valor debe ser único en todas las regiones y, una vez definido, no se debe cambiar.

4. (Todas las regiones) Defina los prefijos adecuados para las solicitudes, los cambios y las incidencias desde Service Desk > Números de secuencias.

El prefijo debe ser único en todas las regiones para cada tipo de ticket (por ejemplo, para las solicitudes). La unicidad de los prefijos facilita la búsqueda de partes en todas las regiones.

5. (Región master) Cree un registro de región master en Regiones globales desde Service Desk, Soporte de varios sitios, Configuración de región master, Regiones globales, y seleccione la casilla de verificación *Master*. A continuación, lleve a cabo los siguientes pasos:
 - a. En Nombre, escriba un nombre fácil de recordar.
 - b. En Nombre global, escriba el valor definido en la opción `global_name`.
 - c. Defina los valores de los prefijos con el valor establecido en el paso 3.
 - d. En Dirección de servidor primario, defina el nombre o la dirección IP del servidor primario de la región.
 - e. En Dirección de servidor Web, defina el nombre o la dirección IP del servidor al que se conectan las demás regiones.
 - f. Confirme la dirección URL del servidor Web (no se debe cambiar).
 - g. En Puerto de servidor Web, defina el número de puerto del servidor Web indicado anteriormente. Este valor debe ser 8080 para la conexión con Tomcat. Si se deja en blanco, se toma el valor del puerto predeterminado para el protocolo de servidor Web.
 - h. En Protocolo de servidor Web, defina la dirección del servidor Web (`http` o `https`) indicada anteriormente.
 - i. Seleccione la casilla de verificación *Master* (sólo en el caso del servidor master).
6. (Región master) Cree otras regiones remotas desde Service Desk, Soporte de varios sitios, Configuración de región master, Regiones globales. Consulte los pasos anteriores de configuración de la región master.

Después de que se crean las otras regiones remotas, ejecute `pdm_extract` en la tabla `Global_Servers` para crear un archivo (por ejemplo, `pdm_extract Global_Servers > gservers.dat`) y copiar el archivo que resulta a una región remota nueva.
7. (Región remota) Ejecute `pdm_load` en los datos de la tabla `Global_Servers` de la región master para cargarlos en la base de datos de la región remota (por ejemplo, `pdm_load -f gservers.dat`). Esto se hace sólo una vez por cada región remota. Después de la conexión, la Región global mantiene esta tabla.
8. (Región master) Defina los nombres de las colas globales desde Service Desk, Soporte de varios sitios, Configuración de región master, Reglas globales.

9. (Todas las regiones) Inicie todas las reglas globales desde Service Desk, Soporte de varios sitios, Configuración de regional local, Reglas globales.
 - a. Haga clic en el botón Mostrar filtro, cambie de Activo a Inactivo y haga clic en el botón Buscar.
 - b. Haga clic en el botón Editar en lista para mostrar los campos correspondientes.
 - c. Cambie de Inactivo a Activo y haga clic en el botón Cambiar todo para que el cambio se aplique a todos los registros.
 - d. Haga clic en el botón Guardar para activar todas las reglas.
 - e. En este momento, se inicia la replicación de todos los datos entre esta región y la master.
10. (Todas las regiones) Asigne los grupos locales a las colas globales desde Seguridad, Grupos. Seleccione o cree el grupo aplicable y defina el campo Cola global con el nombre de la cola global que se debe asignar al grupo.

La configuración de varios sitios ha finalizado.

Definición de las regiones participantes

Las regiones globales definen una serie de regiones que participan en un sistema de varios sitios. Solamente se puede definir una región como la región principal y la región principal como la primera región.

Nota: En el caso de una instalación para varios sitios, si desea utilizar los valores de prefijo, debe definir un prefijo o sufijo para todas las regiones que participan en la instalación de varios sitios. Si define un prefijo para uno de los servidores y no para el resto de los servidores regionales participantes, no podrá buscar tickets globales con el valor del prefijo. Defina los valores del prefijo para todas las regiones participantes o no defina los valores del prefijo para los servidores regionales participantes.

Por razones de seguridad, la región principal controla qué regiones pueden comunicarse con la región principal. Si una región sin definir intenta conectarse con la principal, se omite la solicitud. Las regiones remotas sólo pueden comunicarse con la principal y no entre ellas. Si una región remota intenta comunicarse con otra región remota, como por ejemplo para la omisión de autenticación, la solicitud se envía primero a la región principal. La región principal envía la solicitud a la otra región remota. La respuesta sigue la ruta inversa de vuelta al solicitante.

Importante: todas las regiones que participen en una configuración de varios sitios debe utilizar la misma página de códigos en todos los servidores primarios. De lo contrario, pueden producirse errores de datos.

Procedimiento para definir las regiones participantes

1. En el Gestor de opciones, establezca la opción `global_name` con el nombre para esta región. Por ejemplo, `NA_REGION` es el nombre global para la región de Norteamérica. Este valor debe ser exclusivo de todas las otras regiones; se introduce en el campo Nombre global cuando define regiones que participan en varios sitios de CA Service Desk Manager. No cambie esta opción después de que se haya definido.
 2. Instale la opción y reinicie el servidor de CA Service Desk Manager (obligatorio).
 3. Inicie sesión en la interfaz Web de la región principal como administrador y cree una región global mediante el valor nombre global definido en el gestor de opciones.
 4. Por cada región que no esté definida como la región principal, necesitará extraer una copia del archivo de datos `Global_Servers` de la región principal y cargarlo localmente de la siguiente manera:
 - Ejecute "`pdm_extract Global_Servers > gs.dat`" en el servidor de la región principal después de que se haya agregado la región remota a las regiones globales.
 - Copie el archivo *gs.dat* en la región remota y cárguelo localmente mediante el comando *pdm_load gs.dat*. No necesita reciclar el servidor de CA Service Desk Manager para aplicar los cambios.
- Una vez cargada inicialmente la tabla `Global_Servers`, los cambios realizados en la región principal pasarán a las regiones remotas mediante la regla "Extraer `Global_Servers`", por lo que sólo tendrá que extraer una copia de `Global_Servers` una vez.
5. Verifique que las dos regiones se comuniquen entre sí mediante la comprobación de `stdlog` en los dos sistemas. Busque una entrada de registro como "Se ha unido la región (`region_name`).\" o "Conectado a región principal (`master_region_name`).\"

Activación de reglas

Las reglas de tabla global se utilizan para definir las reglas que controlan las tablas que se van a replicar, en el caso de que se permita, con qué frecuencia se hará y una consulta opcional que se replica para filtrar datos. Las regiones remotas definen cuándo y con qué frecuencia se replican datos desde y hacia la región master. La propia región master define qué regiones pueden comunicarse con la región master.

Las reglas se definen con nombres como reglas de inserción o extracción:

- Las primeras insertan datos en la tabla global pertinente de la región master.
- Las segundas extraen los datos de la tabla correspondiente de la región master y los almacenan en copias locales de la tabla.

Cada regla de inserción tiene su correspondiente regla de extracción, con dos excepciones: los nombres de los servidores globales y de la cola global sólo se definen en la región master, por tanto, no tienen reglas de inserción.

En general, todas las reglas entregadas deben activarse. La región master es una excepción y sólo necesita activar las reglas de inserción. Si se activan reglas de extracción en la región master, se producirá un error y la regla no se ejecutará. Si la región master no es una instalación de CA Service Desk Manager en funcionamiento, no es necesario activar reglas en Master.

Para reducir la replicación de las colas globales, tal vez prefiera replicar sólo los datos de Global_Request_Queue, Global_Change_Queue y Global_Issue_Queue en la región master y no en las regiones remotas. Los analistas que trabajen con colas globales iniciarán sesión en la región master para determinar qué hay en sus colas globales.

De forma predeterminada, todas las reglas están definidas como inactivas. Este estado permite a un administrador elegir qué reglas se pueden ejecutar, con qué frecuencia y si se deben aplicar otros filtros de datos adicionales. La replicación de datos globales ejecuta consultas con una prioridad menor que el resto de CA Service Desk Manager, por lo que la replicación debería poderse ejecutar durante el procesamiento normal de CA Service Desk Manager sin que suponga un gran impacto.

Para cada región que participa en una configuración de varios sitios, realice lo siguiente:

1. Inicie sesión en cada región como Administrador. En la ficha Administración, desplácese hasta Reglas globales en los libros Asistencia multidepartamental y Valores de región local.
2. Defina los criterios de búsqueda Activo como Inactivo y seleccione Buscar.
3. Revise los valores predeterminados de cada regla de la lista, defina el estado como Activo y haga clic en Guardar. Si la programación permite que se ejecute la regla, lo hará inmediatamente.

Cuando se activa o desactiva una regla, el cambio se aplica inmediatamente. Es necesaria una conexión con la región master para que una regla pueda funcionar. Si falla una conexión con la región master, se suspenderá la replicación hasta que se restablezca la conexión.

Configuración de grupos globales

Para presentar información a los usuarios de todos los sistemas que participan en una configuración global, un subconjunto de datos de las tablas Contacto, Organización, Ubicación, Producto, Solicitud, Orden de cambio e Incidencia se recopila en tablas nuevas y más pequeñas. Esta información de resumen se replica periódicamente entre los sistemas que participan para mejorar la eficiencia y el rendimiento. Si el analista necesita ver el resto de datos, puede desplazarse hasta ese sistema para acceder a ellos.

Es necesario definir grupos globales para que la replicación de datos admita las colas globales (Solicitud, Cambio o Incidencia). Sólo los tickets asignados a grupos globales cumplirán los requisitos para la replicación. Una vez que se ha definido una región master, sólo se pueden definir grupos globales en ésta.

Procedimiento para definir un grupo global

1. Navegue a Soporte de varios sitios, Valores de región master, Nombres de cola globales en la ficha Administración de la región master.
2. Haga clic en Crear nuevo.
3. Introduzca el nombre que quiere asignar a esta cola y haga clic en Guardar.

Se crea el grupo de usuarios globales.

Procedimiento para asignar grupos a colas globales

1. Navegue a Seguridad, Contactos de la ficha Administración.
2. Busque el grupo que desee asociar a la cola global y haga clic en Editar.
3. Seleccione el valor de Cola global y haga clic en Guardar.

Todos los futuros tickets asignados a este grupo cumplirán los requisitos para la replicación.

Personalización del proceso de replicación

Es posible personalizar el proceso de replicación para agregar más columnas a tablas existentes o incluso tablas nuevas.

Para todas las personalizaciones de replications de datos, complete las siguientes tareas:

1. Modificar el archivo global_sd.xml (see page 60)
2. Probar el archivo global_sd.xml (see page 63)

Para tablas nuevas, complete los siguientes pasos:

1. Agregar una nueva asignación global (see page 63)
2. Agregar una nueva regla global (see page 64)

Cómo se modifica el archivo global_sd.xml

El archivo global_sd.xml define las tablas disponibles para la replicación y cómo se asignarán entre regiones. El archivo se encuentra en \$NX_ROOT/site/cfg/global_sd.xml, y se utiliza en el proceso pdm_global_nxd. Después realizar cambios al archivo, debe reiniciar los servicios de CA Service Desk Manager para que los cambios tomen efecto.

El archivo global_sd.xml tiene las secciones principales siguientes:

Tablas

Define cada tabla que suministra o acepta los datos como parte del proceso de replicación.

Asignaciones

Define las asignaciones de las tablas que suministran los datos y la tabla que almacena los datos.

No es necesario definir del mismo modo las asignaciones de tabla entre regiones, aunque si son iguales, es más fácil detectar diferencias.

Nota: Es necesario tener experiencia con XML para realizar personalizaciones ya que, una modificación incorrecta del archivo global_sd.xml podría hacer que la replicación deje de funcionar.

Para modificar el archivo global_sd.xml, realice los pasos siguientes:

1. Asegúrese de hacer una copia de seguridad de este archivo antes de hacer cambios.
2. Utilice un editor de texto estándar, como el Bloc de notas de Windows o vi de UNIX.
3. Utilice una definición existente como ejemplo.
4. Guarde los cambios como texto sin formato y no como UNICODE o texto con formato.

Diseño del archivo global_sd.xml

El archivo global_sd.xml tiene las secciones siguientes:

<GlobalMaps>

(Obligatorio) Indica que este XML está reservado para asignación global. No cambiar.

<Tables>

Muestra una lista de las definiciones de las tablas que participan en la replicación.

<Table name="xx" factory="xx">

Ofrece una definición de tabla, formada por varias definiciones de columna.

Nombre

(Obligatorio) Especifica que el nombre tiene que ser el mismo valor definido en el archivo ddict.sch.

Fábrica

(Obligatorio) Especifica el nombre de objeto definido en los archivos .maj o .mod de esta tabla.

<Column name="xx" [primary_key="true"] [update_key="true"] [last_mod_date="true"] [map_to_name="yy"] [set_system_id="true"] [set_id="true"]>

Define una columna en la definición de la tabla.

Nombre

(Obligatorio) Es el nombre real de la columna como se define en ddict.sch para esta tabla.

Primary_key

(Opcional) Indica que esta columna es la clave principal de esta tabla. Sólo puede definirse una columna como primary_key.

Update_key

(Opcional) Indica que esta columna se utilizará en la región de destino para determinar si ya existe una fila. Pueden definirse hasta 2 columnas por tabla como update_key.

Last_mod_date

(Opcional) Indica que esta columna contiene la última fecha de modificación de la fila. Todas las tablas tienen que tener una columna definida como last_mod_date, ya que esta columna determinará principalmente si se ha replicado una fila.

Map_to_name

(Opcional) Permite cambiar el nombre o asignar columnas a una definición de tabla de destino.

Set_system_id

(Opcional) A la hora de insertarse en la región master, esta columna se define como remote_system_id del origen que se define en la tabla Global_Servers de esta región.

Set_id

(Opcional) A la hora de insertarse en la región master, esta columna tendrá un nuevo valor de ID asignado en el master.

<Maps>

Listas que las definiciones de asignación utilizaban en la replicación.

<Map name="xx" direction="ToMaster | FromMaster">

Define una asignación de replicación.

Nombre

(Obligatorio) Define el nombre de esta asignación. En la tabla Global_Table_Map se hace referencia a este nombre como map_definition.

Dirección

(Necesario) Indica la dirección utilizada en esta asignación para replicar datos. ToMaster empuja los datos a la región master. FromMaster obtiene los datos de la región master.

<From_Table table_name="xx">

Define la tabla o tablas de origen de las que se copiarán los datos. Puede haber dos definiciones From_Table en una asignación. Dos definiciones permiten la combinación de datos de dos tablas para formar una tabla de destino.

Table_name

(Obligatorio) Define el nombre de la definición de la tabla. Esta tabla debe estar definida en la sección de tablas anterior.

<To_Table table_name="xx">

Define la tabla de destino de la que se copiarán los datos. Debe haber una de estas entidades por cada asignación.

Table_name

(Obligatorio) Define el nombre de la definición de la tabla. Esta tabla debe estar definida en la sección de tablas anterior.

<Where_Clause clause="xx">

Si dos tablas definen una fuente, esta entidad definirá la cláusula Where utilizada para unir las dos tablas. Debe haber una de estas entidades por cada asignación.

Cláusula

(Obligatoria) Ésta es la cláusula SQL para unir dos tablas. Esta propiedad debe existir, pero puede tratarse de una cadena vacía.

<Order_By table_name="xx" column_name="yy">

Define el orden en el cual las filas se replican. Éste debería registrarse por la última fecha de modificación de From_Table. Debe haber una de estas entidades por cada asignación.

Table_name

(Obligatorio) Es el nombre de tabla de una de las entidades From_Table.

Column_name

(Obligatorio) Es el nombre de columna de Table_name que indica la última fecha de modificación.

Probar el archivo global_sd.xml

Tras realizar cambios en el archivo global_sd.xml, puede comprobar que los cambios son válidos. En la línea de comandos del servidor principal, ejecute el siguiente comando:

```
pdm_global_nxd -x
```

Para ejecutar este comando no es necesario que se estén ejecutando los servicios de CA Service Desk Manager.

Si no se detecta ningún error, aparece el mensaje "No hay errores en el archivo de configuración XML". Si se detectaron errores, aparece el mensaje "Hay errores en el archivo de configuración XML". Consulte el *stdlog* más reciente para obtener una lista de todos los errores.

Si hay errores en el archivo global_sd.xml cuando se inician los servicios de CA Service Desk Manager, no se lleva a cabo replicación alguna. Tras corregir el archivo global_sd.xml, reinicie los servicios para reiniciar la replicación de datos.

Agregar una nueva asignación global

Para que las nuevas asignaciones aparezcan definidas en las reglas, también deben estar definidas en la tabla Global_Table_Map. Esta tabla contiene las asignaciones definidas en el archivo global_sd.xml disponibles para reglas.

Procedimiento para agregar una nueva asignación global

1. Desplácese a Service Desk, Soporte de varios sitios, Configuración regional local, Asignaciones globales.
2. Seleccione Crear nuevo para crear una entrada.
3. Introduzca un nombre y una descripción opcional.

Nota: El campo Definición de asignación debe tener el mismo nombre de asignación que en el archivo global_sd.xml.

4. Haga clic en Guardar.

La asignación global se agrega a la tabla Global_Table_Map.

Reglas globales

Una vez que se ha definido Global_Table_Map en ambas tablas (global_sd.xml y Global_Table_Map), puede utilizarse en una regla global. Puede definir varias reglas globales para una sola asignación global. Múltiples definiciones pueden resultar útiles en las situaciones siguientes:

- Es posible que desee reducir la cantidad de consultas de cambios en las horas punta. Por ejemplo, entre 7:00 a. m. y 10:00 a. m., quiere un intervalo de repetición superior que el necesario durante el resto del día. En tal caso, crearía dos reglas con dos programaciones distintas y dos intervalos distintos.
- Es posible que desee que haya filtros diferentes (consulta adicional) para las distintas reglas. Por ejemplo, desea que se repliquen rápidamente las solicitudes de prioridad 1 y que el resto se repliquen con una frecuencia menor. En ese caso, puede crear dos reglas con una consulta adicional diferente y distintos intervalos.

Puede crear reglas o actualizar reglas existentes en la ficha Administración, desde Service Desk, Soporte de varios sitios, Valores de región local, Reglas globales.

Configuración de zonas de servidor y alias de servidor

Las zonas de servidor y los alias de servidor permiten a los analistas globales acceder a interfaces Web de distintas regiones. Las configuraciones de red y los cortafuegos pueden hacer que no sea posible acceder a los nombres de los servidores o las direcciones IP de todas las ubicaciones. Para solucionar este problema, puede crear un alias de servidor y convertir así un nombre de servidor en otro distinto o en otra dirección IP. Si no se define un alias para una zona de servidor específica, se utilizará el nombre de servidor Web definido para la región global.

Las zonas de servidor permiten definir recopilaciones de alias para su aplicación a diferentes situaciones. De manera predeterminada, las zonas de servidor de Internet o Intranet están disponibles. Sin embargo, es posible renombrarlas o crear zonas. Por ejemplo, se puede crear una recopilación de alias para el acceso a CA Service Desk Manager a través de Intranet y otra recopilación de alias para gestionar el acceso a CA Service Desk Manager a través de Internet. Por tanto, los analistas globales pueden seleccionar una zona de servidor si modifican el valor de Zona activa en sus preferencias Web (menú Service Desk: Ver / Preferencias).

Nota: Las zonas y alias de servidor se definen localmente para la región. Los cambios que se hagan en estas tablas no estarán disponibles para otras regiones.

Procedimiento para crear una zona de servidor

1. Navegue a Soporte de varios sitios, Valores de regional local, Zonas de servidor.
2. Haga clic en Crear nuevo.
3. Introduzca el nombre de la zona que va a definir.
4. (Opcional) Seleccione el valor predeterminado para designar una zona de servidor predeterminada.
5. Haga clic en Guardar.

El sistema crea la zona de servidor.

Procedimiento para crear un alias de servidor

1. Navegue a Soporte de varios sitios, Valores de regional local, Alias de servidor.
2. Haga clic en Crear nuevo.
3. Para dar nombre al alias, introduzca el nombre de servidor que desea sustituir.
4. Seleccione la zona a la que desee que esta entrada de alias se asocie.
5. Para la dirección de host, introduzca el nuevo nombre de host o dirección IP en la que desee que se convierta la zona y haga clic en Guardar.

El sistema crea el alias de servidor.

Actualización de roles para Ir a Recursos

Debe actualizar los Ir a Recursos de los roles cuando se implementa el soporte de varios sitios. Gracias a esto se puede permitir que sólo ciertos roles utilicen tickets globales.

Procedimiento para actualizar un rol para Ir a Recursos

1. Vaya a Gestión de seguridad y de roles, Gestión de roles, Lista de roles. Aparecerá la lista de roles.
2. Haga clic en el nombre de un rol. Por ejemplo, haga clic en Administrador. Aparecerá la página Detalles del rol de administrador.
3. Seleccione la ficha Ir a Recursos y haga clic en Actualizar Ir a recursos.
4. Agregue los Ir a Recursos adecuados para el rol.
5. Haga clic en Guardar.

Ejemplos de varios sitios

Ejemplo 1: Receptor de llamada global: nueva solicitud.

Mientras consulta el perfil rápido global, el analista recibe una llamada de un cliente. Éste introduce el criterio de búsqueda para localizar al cliente y hace clic en Buscar. El analista utiliza la información proporcionada en la lista para seleccionar la fila de contacto adecuada. Los campos Contacto seleccionado y Sistema remoto se rellenan automáticamente y se activa el botón Salto a sistema de contacto. El analista rellena opcionalmente el campo Bloc de notas y hace clic en Crear solicitud. Se abre un nuevo formulario de solicitud con el nombre y la descripción del contacto introducidos a partir de la información del bloc de notas. El analista procesa la solicitud con normalidad y hace clic en Guardar para crear una nueva solicitud.

Ejemplo 2: Receptor de llamada global: solicitud existente.

Mientras consulta cualquier formulario, incluyendo el perfil rápido global, el analista recibe una llamada de seguimiento para el número de solicitud NA:1234. El analista introduce NA:1234 al lado del botón Ir, selecciona Solicitudes globales y hace clic en Ir. Aparece la solicitud de la región remota o local, y el analista puede procesar la solicitud de manera normal.

Ejemplo 3: Analista global: cola de solicitudes globales de proceso

Un analista asociado a un grupo global configura su panel de resultados con una consulta almacenada que muestra sólo sus solicitudes globales. Si selecciona un elemento del panel de resultados, se mostrarán las solicitudes de la consulta almacenada en el panel derecho del explorador. Si selecciona uno de los elementos de la lista, se mostrarán los detalles de la solicitud del sistema en el que se creó la solicitud.

Multicliente

Multicliente es la capacidad que poseen varios clientes independientes (y sus usuarios) de compartir una única implementación de CA Service Desk Manager. Los usuarios de cliente solamente interactúan el uno con el otro de maneras definidas, según lo especificado por su *roles y jerarquías de clientes*. Típicamente, a menos que le conceda acceso un rol o jerarquía, cada cliente ve la implementación de CA Service Desk Manager únicamente para su propio uso y no puede actualizar ni ver los datos de otro cliente.

Multicliente admite que los clientes compartan recursos de soporte de aplicaciones y hardware, lo cual reduce el coste de los dos, mientras obtiene muchos beneficios de una implementación independiente.

Nota: Para obtener información sobre la instalación y configuración multicliente, consulte la *Guía de implementación*.

Proveedor de servicio

El *proveedor de servicios* es el cliente primario (propietario) en una instalación de multicliente de CA Service Desk Manager. El primer cliente agregado a una instalación de CA Service Desk Manager es siempre el cliente proveedor de servicios. El cliente proveedor de servicios no puede tener un cliente superior.

CA Service Desk Manager asocia el usuario privilegiado (típicamente ServiceDesk en Windows o srvcdesk en Linux/UNIX) con el cliente proveedor de servicios.

Solamente el cliente proveedor de servicios puede ejecutar cualquiera de las siguientes tareas de CA Service Desk Manager:

- Definir las opciones de CA Service Desk Manager
- Definir las opciones de Gestión del conocimiento
- Definir las opciones de Automatización de soporte
- Crear tablas o columnas

- Crear, editar o suprimir clientes
- Permitir que los clientes tengan subclientes
- Actualizar datos públicos

Nota: Un administrador puede conceder a los usuarios cliente acceso a los datos que no son suyos. Los analistas de clientes que no son proveedores de servicios pueden tener solamente acceso a sus propios clientes y subclientes, a menos que su acceso de función se actualice para incluir al cliente del analista. Por ejemplo, una definición de roles puede establecer un acceso separado de lectura y escritura a ciertos grupos de clientes para usuarios de ese rol.

Importante: se establece al primer cliente creado como el proveedor de servicios; después de eso, la casilla de verificación Proveedor de servicios y el campo Estado del registro son de sólo lectura.

Más información:

[Administración de proveedores de servicios](#) (en la página 68)

[Acceso del cliente](#) (en la página 71)

[Creación de clientes](#) (en la página 82)

Administración de proveedores de servicios

El proveedor de servicios puede permitir que los clientes administren su propia configuración. Los administradores de clientes tienen acceso a un subconjunto de tareas de administración que es el mismo para todos los clientes, de modo que la tabla ADMIN_TREE no es de cliente. En cambio, el rol de administrador de clientes predeterminado define las funciones de administración que están disponibles para los administradores de clientes.

Para designar a un usuario como un administrador de clientes, seleccione el administrador de clientes para el rol de ese usuario.

Cómo funciona multicliente

Cuando el multicliente está activo, puede conceder cada acceso de contacto a todos los clientes (público), a un cliente solo o a un grupo de clientes (definido por el usuario o mantenido por el producto). El rol de un contacto contra el acceso, que especifica acceso de lectura y escritura independientemente. Dado que el acceso de cliente depende del rol y un contacto puede cambiar roles durante una sesión, el acceso de cliente de contacto también puede cambiar.

Si se instala el multicliente, la mayor parte de los objetos de CA Service Desk Manager incluyen un atributo de cliente que especifica qué cliente posee el objeto. Los objetos recaen en tres grupos, dependiendo de su atributo de cliente y cómo se utilizan:

Sin cliente

Define objetos sin un atributo de cliente. Todos los datos en estos objetos son públicos.

Ejemplos: prioridad y urgencia.

Cliente necesario

Define objetos con un atributo de cliente que no puede ser nulo (impuesto por CA Service Desk Manager, no el DBMS). Todos los datos en estos objetos se asocian con clientes individuales; no hay datos públicos.

Ejemplos: tablas de ticket (Solicitud, Incidencia y Orden de cambio).

Cliente opcional

Define objetos con un atributo de cliente que puede ser nulo. Parte de los datos en estos objetos son públicos, y algunos se asocian con clientes específicos. La vista de cada cliente del objeto es una vista que combina los datos públicos y los datos específicos de cliente.

Ejemplos: categoría y ubicación.

Cuando un usuario consulta la base de datos, CA Service Desk Manager limita los resultados a objetos que pertenecen a clientes a los que el usuario está autorizado a acceder. Esta restricción se aplica además de las restricciones de partición de datos que están en efecto. Esto significa que nunca ve datos en clientes necesarios y tablas opcionales de clientes, excepto los datos que pertenecen a los clientes a los que se les permite acceder.

Cuando un usuario de cliente pide crear o actualizar un objeto de base de datos, CA Service Desk Manager verifica que el objeto pertenezca a un cliente que el rol actual del usuario pueda actualizar, y que todas las referencias de clave externa (SREL) del objeto y otros objetos son para objetos públicos (sin clientes); para objetos del mismo cliente o para objetos de clientes que estén por encima del cliente del objeto en la jerarquía de clientes. Es decir, se permite que un objeto de cliente haga referencia a objetos que le pertenecen a su cliente principal, al cliente principal de su cliente principal y así sucesivamente.

Si un usuario que crea un objeto tiene acceso de actualización a varios clientes, el usuario debe especificar el cliente explícitamente; o directa o indirectamente.

Nota: Hay una excepción a la restricción de referencia de SREL. Ciertas referencias de SREL (como el asignatario de un incidente) pueden referenciar objetos que pertenecen a clientes de la jerarquía de clientes que contiene su objeto. Tales referencias se designan como SERVICE_PROVIDER_ELIGIBLE en el esquema de objetos de CA Service Desk Manager (Majic). El indicador SERVICE_PROVIDER_ELIGIBLE representa una diferencia solamente si el cliente proveedor de servicios no está en la jerarquía de clientes arriba del cliente del objeto; si el cliente proveedor de servicios está en la jerarquía, las reglas de validación del cliente permiten las referencias del proveedor de servicios.

Un usuario proveedor de servicios que solicita crear o actualizar un objeto está sujeto a las mismas restricciones que los usuarios cliente, excepto que los usuarios proveedores de servicios estén autorizados a crear o actualizar objetos públicos. El rol activo del usuario proveedor de servicios controla esta autorización.

Nota: Si CA Service Desk Manager impide que un usuario actualice los datos de clientes, un mensaje de error puede anunciar una limitación de partición de datos. Si recibe este mensaje de error, la partición de datos o las restricciones de multicliente están en efecto.

Opción Multicliente

Multicliente se activa al instalar una de las opciones multicliente siguientes:

- **desactivado:** Multicliente no está en uso. Las funciones de multicliente no están disponibles y los objetos no tienen un atributo de cliente. Esta opción es la configuración predeterminada en una nueva instalación de CA Service Desk Manager.
- **instalación:** las funciones de multicliente están en efecto para los administradores, de modo que los objetos relacionados con el cliente y los atributos sean visibles y editables. Sin embargo, CA Service Desk Manager no exige restricciones de cliente y los usuarios que no son administradores no ven cambio alguno. Esta configuración permite que un administrador se prepare para la opción de multicliente ejecutando tales tareas como clientes que definen; o asignando objetos a clientes sin impactar en el uso normal de CA Service Desk Manager.
- **activado:** Multicliente está plenamente operativo. Todos los usuarios ven los cambios en la interfaz de usuario apropiada para ellos y CA Service Desk Manager exige restricciones de cliente.

Nota: Para obtener más información acerca de la instalación e implementación multicliente, incluyendo las opciones adicionales para su aplicación, consulte la *Guía de implementación*.

Información de clientes

Crea y actualiza clientes cuando instala multicliente (en el modo de aplicación instalación u obligatoriedad total). La información conservada para un cliente es similar a los datos conservados para una organización, excepto los siguientes dos atributos:

Logotipo

Proporciona una URL a un archivo de imagen con el logotipo del cliente. El logotipo se muestra en la página Detalles de cliente misma y como sustituto del logotipo de CA en los formularios Web mostrados por un usuario de cliente; o bien, se muestra un objeto asociado con el cliente.

Proveedor de servicio

Indica si el cliente es el proveedor de servicios. El cliente proveedor de servicios es siempre el primer cliente agregado. Cuando el administrador agrega al primer cliente, ocurre lo siguiente:

- El primer cliente se convierte en proveedor de servicios. Esta designación no se puede cambiar.
- El usuario con privilegios (generalmente ServiceDesk) y todos los contactos de sistema (como System_AHD_Generated) están definidos como pertenecientes al cliente de proveedor de servicios nuevo

Nota: El usuario del sistema "administrador" se agrega en Windows solamente y no se le asigna a un cliente. El usuario con privilegios debe asignar un cliente como Administrador de forma manual.

Acceso del cliente

El rol de un usuario de CA Service Desk Manager domina tanto la autorización de acceso como la interfaz de usuario. El conjunto de roles disponibles para usuarios dependen de su tipo de acceso. El multicliente le permite controlar el cliente o grupo de clientes al que un usuario puede acceder dentro del rol.

La página Detalles de rol proporciona las listas despegables Acceso del cliente y Acceso de escritura del cliente en la ficha Autorización. Acceso del cliente es sólo de visualización y Acceso de escritura del cliente permite crear y actualizar.

Puede asignar a roles las asociaciones siguientes:

Igual que el acceso de clientes (Acceso de escritura del cliente solamente)

Establece el acceso de escritura del cliente para que sea el mismo que la configuración Acceso del cliente. Es el valor predeterminado y válido solamente para Acceso de escritura del cliente.

Todos los clientes

Elimina restricciones de clientes. CA Service Desk Manager permite que un usuario en un rol con este acceso pueda ver cualquier objeto en la base de datos (acceso de lectura) o crear y actualizar (acceso de escritura) cualquier objeto de cliente en la base de datos. Cuando los usuarios con el acceso Todos los clientes crean un objeto, CA Service Desk Manager exige que seleccionen al cliente del nuevo objeto.

Un solo cliente

Establece el acceso de cliente de un rol en un cliente nombrado. Cuando esta opción se selecciona, aparece un segundo campo en la interfaz de usuario Web que permite la selección de un cliente específico. CA Service Desk Manager limita a un usuario en un rol con este acceso para que vea (acceso de lectura) o cree y actualice (acceso de escritura) solamente esos objetos asociados con el cliente nombrado. Esta selección es válida tanto para el Acceso del cliente como para el Acceso de escritura del cliente.

Grupo de clientes

Establece el acceso de cliente de un rol a un grupo de clientes mantenido por el sistema o definido por el usuario. Cuando esta opción se selecciona, aparece un segundo campo en la interfaz de usuario Web que permite la selección de un grupo de clientes específico. CA Service Desk Manager limita un usuario con el rol para ver (acceso de lectura) o crear y actualizar (acceso de escritura) solamente esos objetos asociados con uno de los clientes del grupo. Cuando un usuario con el acceso de grupo de clientes crea un objeto, CA Service Desk Manager exige que seleccionen al cliente para el nuevo objeto. Esta selección es válida tanto para el Acceso del cliente como para el Acceso de escritura del cliente.

Cliente del contacto

Establece el acceso de cliente de un rol al cliente del contacto que lo utiliza. CA Service Desk Manager limita a un usuario en un rol con este acceso para que vea (acceso de lectura) o cree y actualice (acceso de escritura) solamente esos objetos asociados con su propio cliente. Esta selección es válida tanto para el Acceso del cliente como para el Acceso de escritura del cliente.

Grupo de clientes del contacto (Analista solamente)

Establece acceso de rol de un analista al grupo de clientes con el cual trabaja el analista, según lo especificado en el registro de contacto del analista. Si el usuario con el rol no es un analista, esta selección tiene el mismo efecto que el cliente del contacto. Esta selección es válida tanto para el Acceso del cliente como para el Acceso de escritura del cliente.

Grupo de subclientes del contacto

Establece el acceso de cliente de un rol al grupo de subclientes del contacto que lo utiliza. CA Service Desk Manager limita a un usuario en un rol con este acceso para que vea (acceso de lectura) o cree y actualice (acceso de escritura) solamente esos objetos asociados con su propio grupo de subclientes. Esta selección es válida tanto para el Acceso del cliente como para el Acceso de escritura del cliente.

Grupo de superclientes del contacto

Establece el acceso de cliente de un rol al grupo de superclientes del contacto que lo utiliza. CA Service Desk Manager limita a un usuario en un rol con este acceso para que vea (acceso de lectura) o cree y actualice (acceso de escritura) solamente esos objetos asociados con su propio grupo de superclientes. Esta selección es válida tanto para el Acceso del cliente como para el Acceso de escritura del cliente.

Grupo de clientes relacionados del contacto

Establece el acceso de cliente de un rol al grupo de clientes relacionados del contacto que lo utiliza. CA Service Desk Manager limita a un usuario en un rol con este acceso para que vea (acceso de lectura) o cree y actualice (acceso de escritura) solamente esos objetos asociados con su propio grupo de clientes relacionados. Esta selección es válida tanto para el Acceso del cliente como para el Acceso de escritura del cliente.

Todos los usuarios pueden ver datos públicos, sin tener en cuenta los derechos de acceso de su rol actual. La casilla de verificación Actualizar datos públicos controla si un usuario proveedor de servicios en el rol tiene la autorización para crear o actualizar datos públicos. Los usuarios de cliente (usuarios que le pertenecen a un cliente que no sea el proveedor de servicios) no pueden actualizar datos públicos, independientemente de su rol.

Más información:

[Edición del acceso de cliente para un rol](#) (en la página 74)

Edición del acceso de cliente para un rol

Es posible asignar o editar el acceso de cliente para un rol.

Procedimiento para editar el acceso de cliente para un rol

1. Vaya a Gestión de seguridad y de roles, Gestión de roles, Lista de roles.
Aparecerá la lista de roles.
2. Haga clic en un rol.
Aparecerá la página Detalles del rol.
3. Haga clic en Editar.
Aparecerá la página Actualizar rol.
4. Seleccione las opciones para Acceso de cliente y Acceso de escritura del cliente.

Nota: Tenga cuidado si selecciona opciones diferentes para esta configuración.

5. Haga clic en Guardar.

Las opciones actualizadas de acceso de cliente se guardan para el rol.

Términos de uso del cliente

Una declaración de términos de uso presenta al usuario final una declaración de página inicial cuando éste inicia sesión en CA Service Desk Manager. La declaración le recuerda al usuario sobre el uso apropiado del producto. El usuario debe aceptar los términos antes de que pueda proceder a iniciar sesión en CA Service Desk Manager. Las entradas se escriben en el registro estándar y en el registro de eventos del usuario después del intento de inicio de sesión.

Puede ejecutar las siguientes acciones de términos de uso:

- Crear, actualizar y suprimir una declaración de términos de uso.
- Asociar una declaración de términos de uso con un cliente.

Nota: Debe habilitar la opción multicliente y configurar uno o más clientes para poder asociar una declaración de términos de uso con un cliente.

- Exigir al usuario final que acepte la declaración cada vez que inicie sesión.
- Permitir que el usuario final omita la declaración inicial presentando una declaración de términos de uso en blanco.

Más información:

[Cómo configurar los términos de uso](#) (en la página 75)

Cómo configurar los términos de uso

La declaración de términos de uso presenta al usuario final una declaración de página inicial cuando éste inicia sesión en CA Service Desk Manager. La declaración le recuerda al usuario sobre el uso apropiado del producto. El usuario debe aceptar los términos antes de que pueda proceder a iniciar sesión en CA Service Desk Manager. Si el usuario final selecciona Aceptar, CA Service Desk Manager prosigue con el inicio de sesión y muestra el formulario principal. Si el usuario selecciona Rechazar, CA Service Desk Manager vuelve al inicio de sesión. Las entradas se escriben en el registro estándar y en el registro de eventos del usuario después del intento de inicio de sesión.

Normalmente, puede configurar los términos de cliente de contacto de la declaración de uso. Si el cliente de contacto se configura con una declaración de términos de uso inactiva, no se configuran los términos de uso, o si se selecciona <vacío> en la lista desplegable Términos de uso, CA Service Desk Manager muestra los términos de declaración de uso para los principales de clientes, los principales de los principales, etc. Si no se encuentra ninguna declaración de términos de uso en ningún nivel, CA Service Desk Manager prosigue con el inicio de sesión. Si configura un cliente con una declaración de términos de uso en blanco, CA Service Desk Manager prosigue con el inicio de sesión y muestra el formulario principal.

Puede configurar términos de uso como sigue:

1. Habilite el multicliente.
2. Configure uno o más clientes.
3. Defina una declaración de términos de uso.
4. Actualice un cliente para utilizar la declaración de términos de uso específica.

Nota: Para obtener información detallada sobre cómo crear y modificar declaraciones de términos de uso, consulte la *Ayuda en línea*.

Impacto de la interfaz de usuario

La instalación de la función multicliente cambia la interfaz de usuario, dependiendo de la autorización y el acceso de cliente asociado con el rol del usuario. Los cambios afectan tanto a usuarios de cliente como usuarios proveedores de servicios.

Usuarios de clientes

Si el rol de un usuario está restringido a un cliente solo y el usuario no es administrador, puede sustituir un logotipo personalizado del cliente por el logotipo de CA predeterminado en todas las páginas. Esta sustitución depende de si un logotipo se define en la página Detalles de cliente para el cliente, de modo que es opcional por cliente.

El único cambio de interfaz de usuario para usuarios de cliente que no son administrador es cambiar los elementos de menú o botones que permiten actualizar o editar (el botón Editar o el botón Crear nuevo en una página de lista) por objetos públicos, porque los usuarios de cliente no están autorizados a actualizar un objeto público.

Administradores de clientes

Los administradores de cliente con acceso de un sólo cliente que ven objetos opcionales de cliente observarán un cambio diferente en la interfaz. Las páginas de lista para estos objetos automáticamente incluyen una columna Público que especifica si las filas de lista son datos públicos. Además, el primer elemento en el filtro de búsqueda es una lista desplegable Datos públicos que contiene las selecciones siguientes:

- Incluir (predeterminado)
- Excluir
- Sólo

Un administrador de cliente con el acceso a varios clientes observa una columna Cliente en las páginas de lista para cualquier objeto de cliente. Esta columna toma el lugar de la columna Público en las listas de tablas opcionales de cliente.

Usuarios que pueden ver un grupo de clientes

Si el rol de un usuario permite acceso de lectura a varios clientes o un usuario proveedor de servicios tiene la autorización para actualizar datos públicos, los formularios de lista de CA Service Desk Manager cambian del siguiente modo:

Objetos sin cliente

Los objetos sin cliente contienen solamente datos públicos. Un usuario proveedor de servicios puede crear o actualizar un objeto sin cliente solamente si su rol tiene la autorización para actualizar datos públicos. De lo contrario, la interfaz de usuario suprime elementos de menú o botones que permiten actualizar o editar, como el botón Editar o el botón Crear nuevo en una página de lista. Los usuarios de cliente no pueden actualizar objetos públicos, y estos usuarios nunca ven un botón Editar o Crear nuevo en una página de lista para un objeto sin cliente.

Objetos necesarios de cliente

Los objetos que requieren cliente contienen solamente datos asociados con un cliente concreto. Los formularios de lista para estos objetos automáticamente incluyen una columna Cliente después de la última columna de vínculo. Además, el filtro de búsqueda contiene un selector de cliente que permite que el usuario restrinja una lista a un cliente solo.

Objetos opcionales de cliente

Los objetos opcionales de cliente contienen datos tanto públicos como específicos de cliente. Los formularios de lista para estos objetos incluyen automáticamente una columna Cliente (un cliente vacío indica un objeto público). Además, el filtro de búsqueda contiene tanto un selector de clientes como una lista desplegable Datos públicos (la misma que ven los administradores de cliente).

Nota: Si las tablas necesarias de cliente incorrectamente contienen datos sin cliente en un sistema de multicliente, aparece una lista desplegable de datos públicos en las tablas necesarias de cliente y recibe el mensaje siguiente: "AHD05358 Habían nn objetos sin cliente activos xxx objetos en inicio de Service Desk".

Usuarios que pueden actualizar varios clientes

Si el rol del usuario permite el acceso a varios clientes o el rol de usuario de un proveedor de servicios tiene la autorización para actualizar datos públicos (típico de un analista que trabaja para un proveedor de servicios), las páginas de detalles cambian del siguiente modo:

Objetos sin cliente

Los objetos sin cliente contienen solamente datos públicos. No hay cambios a las páginas de detalles para un usuario proveedor de servicios con la autorización para actualizar datos públicos. Si el usuario está en un rol sin autorización para actualizar datos públicos o no pertenece al proveedor de servicios, las páginas de sólo lectura para los objetos sin cliente no tienen el botón Editar.

Objetos necesarios de cliente existentes

Los objetos que requieren cliente contienen solamente datos asociados con un cliente concreto. Las páginas de detalles para objetos necesarios de cliente existentes muestran el cliente del objeto como parte del encabezado de la página estándar.

Objetos opcionales de cliente

Los objetos opcionales de cliente contienen datos tanto públicos como específicos de cliente. La página de detalles para estos objetos depende de si el usuario pertenece al proveedor de servicios y si está en un rol con la autorización para actualizar datos públicos:

- Si el rol de un usuario proveedor de servicios tiene la autorización para actualizar datos públicos, la página de detalles es la misma que la de los objetos necesarios de cliente.
- Si el rol del usuario no tiene la autorización para actualizar datos públicos o el usuario no pertenece al proveedor de servicios, las páginas de detalles para objetos públicos no tienen un botón Editar. Otras páginas de detalles son las mismas que las de objetos necesarios de cliente.

Impacto de Automatización de soporte

El impacto de multicliente sobre su entorno de compatibilidad depende de las restricciones de rol y cliente impuestas a los usuarios finales y analistas. El proveedor de servicios gestiona los permisos de lectura/escritura para los datos tanto públicos como específicos del cliente. Por ejemplo, un analista puede controlar sesiones de asistencia de la cola pública y una cola específica del cliente, pero sólo puede utilizar herramientas de asistencia en vivo habilitadas para cada cliente.

Para los usuarios finales con acceso a Automatización de soporte, no configure al usuario final para que tenga acceso a un cliente que no es un subcliente del cliente con propiedad sobre el usuario final, a menos que el grupo de claves externas (FK) esté alterado para incluir al cliente con propiedad. Si el usuario final selecciona a un cliente de inicio de sesión o recibe una invitación por medio de un ticket en un cliente que no cumple con este criterio, recibe un error cuando intenta acceder al cliente del usuario final de Automatización de soporte. Esta restricción no se aplica si el cliente con propiedad sobre el usuario final es el cliente del proveedor de servicios.

Para los analistas con acceso a Automatización de soporte, no configure al analista para que tenga acceso de escritura a un cliente que no es un subcliente del cliente con propiedad sobre el analista, a menos que el grupo de claves externas (FK) esté alterado para incluir al cliente con propiedad. Si el analista intenta controlar a un usuario final o invitar a un usuario final desde un ticket, en un cliente que no cumple con estos criterios, obtendrá un error.

Los analistas y los usuarios finales sin acceso de lectura a su cliente no pueden iniciar el cliente de Automatización de soporte. Para los analistas, aparece un mensaje de advertencia en CA Service Desk Manager en este caso, al igual que el de la ficha principal de Automatización de soporte.

Puede utilizar los roles siguientes para gestionar usuarios de Automatización de soporte:

Analista de Automatización de soporte

Proporciona compatibilidad con usuarios finales mediante la asistencia en vivo. El proveedor de servicios determina el acceso de cliente apropiado y puede habilitar herramientas de la asistencia en vivo y acceso de lectura/escritura para tareas automatizadas.

Importante: si un analista que no sea de un proveedor de servicios ha escrito acceso a un cliente principal, intermedio o no relacionado, se debe actualizar el acceso de función para ese cliente. Los analistas sin acceso de lectura a su cliente no pueden iniciar el cliente de analista de Automatización de soporte y aparece un mensaje de advertencia en CA Service Desk Manager, como de la ficha principal de Automatización de soporte principal o un ticket.

Administrador de Automatización de soporte

Configura el entorno de Automatización de soporte para analistas y usuarios finales. El proveedor de servicios determina su acceso de cliente y le permite ver una lista desplegable de clientes en formularios de lista y detalles. Estos formularios le permiten seleccionar clientes específicos o datos públicos al buscar, crear y modificar datos de Automatización de soporte en un entorno multicliente.

Nota: Los objetos como colas, niveles de privacidad y conversaciones preestablecidas son clientes opcionales.

Impacto de Gestión del conocimiento

El impacto de la opción multicliente en su entorno de conocimiento depende de las restricciones de cliente que se coloquen en los usuarios:

Usuarios de clientes

Sustituye el logotipo del cliente por el predeterminado, si el rol está restringido a un cliente solo.

Administradores de clientes

Permite que los administradores vean datos tanto públicos como específicos de cliente. Las páginas de lista para estos objetos automáticamente incluyen una columna Público que especifica si las filas de lista son datos públicos.

Al buscar el conocimiento, el filtro contiene una lista desplegable Datos públicos con selecciones de Incluir (predeterminado), Excluir y Sólo.

Nota: Los objetos como plantillas de proceso de aprobación, categorías, documentos, archivos y foros son cliente opcional.

Categorías de conocimiento y documentos

Los documentos de conocimiento y las categorías de conocimiento son cliente opcional. Considere la información siguiente para objetos de cliente opcional y públicos:

- Los documentos públicos de conocimiento se pueden agregar solamente bajo Categorías de conocimiento públicas.
- Las categorías públicas de conocimiento se pueden agregar solamente bajo categorías públicas.
- Las categorías de cliente se pueden agregar bajo categorías públicas y bajo categorías de un cliente.
- Se pueden agregar solamente documentos de cliente bajo categorías de cliente.
- Se pueden agregar documentos públicos y de cliente bajo categorías públicas.

Nota: La funcionalidad de categoría Cortar/Copiar/Pegar está permitida solamente si la fuente y el destino tienen el mismo cliente, o si el destino es público.

Se definen repositorios como cliente opcional, así el administrador puede crear repositorios diferentes para clientes diferentes.

Las imágenes incrustadas están permitidas solamente cuando se establecen el documento y la imagen al mismo cliente. Se definen también carpetas de datos adjuntos, datos adjuntos y Datos adjuntos a vínculos de documentos como cliente opcional.

Clasificación de preguntas frecuentes

Al ver la clasificación de preguntas frecuentes para usuarios de cliente, considere la información siguiente sobre los documentos públicos:

- Una audiencia más grande que los usuarios de cliente ve los documentos públicos.

La clasificación de preguntas frecuentes de los documentos públicos es más alta que el documento específico de un cliente.

- Cada cliente tiene necesidades diferentes, de modo que los patrones de uso son diferentes entre clientes.

Las mejores soluciones de la página principal de autoservicio de CA Service Desk Manager muestran los cinco mejores documentos públicos, así como los cinco mejores documentos de un cliente.

Puede configurar las mejores soluciones; para ello, vaya a Conocimiento, Estudio de soluciones, Valores de preguntas frecuentes en la ficha Administración.

Tarjeta de informes de conocimientos

La tarjeta de informes de conocimiento permite que los analistas y administradores vean varias métricas como creación de documentos, publicación, coincidencias y votos. Este informe es para un periodo predeterminado, por analista, categoría y organización.

Al utilizar la tarjeta de informes de conocimiento para proporcionar información para un rol que tiene acceso de un sólo cliente, los datos son limitados por los criterios de cliente.

Cómo usar la opción multicliente

Utilice los procedimientos siguientes para administrar las funciones de multicliente de CA Service Desk Manager.

Visualización de clientes

Puede ver clientes de cualquier Lista de cliente.

Nota: Esta opción está disponible solamente si el multicliente está instalado (en modo activo o de instalación).

Procedimiento para ver un cliente

1. En la ficha Administración, seleccione Gestión de seguridad y de roles.
2. Haga clic en Clientes.
Aparecerá la Lista de clientes.
3. (Opcional) Seleccione un cliente de la Lista de clientes.
Aparecerá la página Detalles de cliente.

Nota: Las listas de cliente también se muestran en páginas como Detalles de grupo de clientes y Clientes afectados por elemento de configuración.

Creación de clientes

Puede utilizar el producto para crear a un cliente.

Procedimiento para crear un cliente

1. Seleccione Gestión de seguridad y de roles, Clientes en la ficha Administración.
Aparecerá la página Lista de clientes.

Nota: La opción Gestión de seguridad y de roles, Clientes está disponible solamente cuando la función multicliente está instalada (ya sea activada o configurada).

2. Haga clic en Crear nuevo.
Aparece la página Crear nuevo cliente.
3. Complete los campos editables si es necesario:

Nombre

Muestra el nombre del cliente.

Proveedor de servicio

Identifica si un cliente es el proveedor de servicios. El primer cliente creado es siempre el proveedor de servicios.

Número de cliente

(Información solamente) Muestra el número de cliente. Este campo no es utilizado por CA Service Desk Manager.

Estado de registro

Establece el cliente como activo o inactivo.

Cliente principal

Especifica otro cliente por encima de este cliente, convirtiéndolo en *subcliente* en una jerarquía de clientes.

Subclientes permitidos

Permite que este cliente tenga subclientes. El cliente no puede modificar la configuración.

Profundidad de cliente

(Información solamente) Indica la profundidad de cliente de este cliente.

Grupo de superclientes

(Información solamente) Identifica el grupo de clientes mantenido por el sistema que contiene a este cliente y a todos los clientes por encima de él en la jerarquía de clientes.

Grupo de subclientes

(Información solamente) Identifica el grupo de clientes mantenido por el sistema que contiene a este cliente y a todos los clientes por debajo de él en la jerarquía de clientes.

Grupo de claves externas

(Información solamente) Identifica el grupo de clientes mantenido por el sistema que contiene clientes a los cuales se pueden hacer referencia de un SREL en datos de este cliente. El grupo de clave externa es el mismo que el grupo de superclientes.

Grupo de clientes relacionados

(Información solamente) Identifica el grupo de cliente mantenido por el sistema que consiste en el grupo de superclientes y subclientes para este cliente.

Términos de uso

Especifica la declaración de los términos de uso para el cliente.

Logotipo

Especifica la dirección URL para el archivo de logotipo de cliente, que puede ser cualquier tipo de imagen Web.

Ubicación

Muestra la página Búsqueda de ubicación.

Contacto

Muestra la página Búsqueda de contacto.

Nota: Si ningún contacto se asocia con el cliente respectivo, los campos Dirección de correo electrónico y Dirección de correo electrónico de localizador están inactivos.

4. Haga clic en Guardar.
Se crea el cliente.
5. Cierre la ventana.
6. Haga clic con el botón secundario en la lista de clientes y haga clic en Actualizar.
La lista de clientes se actualiza y muestra el cliente creado.
7. (Opcional) Para asignar este cliente a grupos de clientes definidos por el usuario, haga clic en Actualizar grupos de clientes en la ficha Grupos de clientes.

Edición de un cliente

Puede editar un cliente en la ficha Administración.

Nota: Esta opción está disponible solamente si el multicliente está instalado (en modo activo o de instalación).

Procedimiento para editar un cliente

1. En la ficha Administración, seleccione Gestión de seguridad y de roles.
2. Haga clic en Clientes.
Aparecerá la Lista de clientes.
3. Haga clic con el botón secundario en un cliente y, a continuación, en Editar.
Aparecerá la página Actualizar cliente.
Nota: Cuando edita un cliente existente, aparecen las fichas Subclientes y Elementos de configuración.
4. Realice las modificaciones adecuadas y haga clic en Guardar.
5. Cierre la página Actualizar cliente.
Aparecerá la Lista de clientes.
6. Haga clic con el botón secundario y seleccione Actualizar.
Aparecerá la Lista de clientes actualizada.

Jerarquías de clientes

Una *jerarquía de clientes* es un grupo de clientes estructurado creado o modificado por el sistema cuando se asigna un *cliente principal* a un cliente. El cliente se convierte en un *subcliente* de los clientes (si los hubiera) principales y en la parte superior de dicha jerarquía.

Nota: El proveedor de servicios puede crear varias jerarquías sin relación, o ninguna. Incluso en un sistema con jerarquías de clientes, es posible definir clientes independientes.

Un subcliente normalmente representa una subdivisión dentro de sus *superclientes*. Un subcliente puede tener sus propios datos y reglas de negocio, y los datos del supercliente se "insertan" automáticamente en el subcliente como de sólo lectura.

CA Service Desk Manager admite una jerarquía de clientes de profundidad ilimitada. Sin embargo, el *proveedor de servicios* puede especificar un límite en el número total de clientes y la profundidad de jerarquías de clientes (el valor predeterminado es cuatro niveles). El proveedor de servicios también determina si los clientes individuales pueden tener subclientes.

Nota: El proveedor de servicios puede participar en jerarquías de clientes, pero esto no es obligatorio. El proveedor de servicios no puede tener un cliente principal.

Creación de subclientes

Con los subclientes puede construir y modificar las jerarquías de clientes con fines organizativos y para compartir datos. Para situar a un cliente en una jerarquía de clientes, debe asignarle la categoría de cliente principal.

Para crear un subcliente

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Clientes.

Aparecerá la Lista de clientes.

Nota: La opción Gestión de seguridad y de roles, Clientes está disponible solamente cuando se habilita el multicliente.

2. Haga clic en un cliente existente para editarlo, o haga clic en Crear nuevo.
Aparecerá la página Detalles de cliente. Introduzca cualquier dato o cambio que sea necesario.

3. Seleccione un cliente principal.

Nota: La lista desplegable Cliente principal solo muestra clientes que pueden tener subclientes.

4. Haga clic en Guardar.

El cliente es un subcliente del cliente principal.

Nota: Cuando un cliente es un subcliente, pertenece al grupo de subclientes del cliente principal, al igual que los subclientes (si los hubiere) de ese subcliente, y así sucesivamente. El cliente principal se une al grupo de superclientes del subcliente, al igual que los superclientes (si los hubiere) de ese supercliente, y así sucesivamente. Cada uno se une al grupo de clientes relacionados del otro.

Grupos de clientes mantenidos por el sistema

CA Service Desk Manager genera y mantiene tres grupos de cliente automáticamente para cada cliente de una jerarquía de clientes (*tenant* es el nombre del cliente):

- *tenant_subtenants* (cliente, sus clientes secundarios y sus subclientes más bajos)
- *tenant_supertenants* (cliente, su cliente principal y sus superclientes más altos)
- *tenant_relatedtenants* (toda la jerarquía exclusiva)

Los grupos de clientes mantenidos por el sistema se pueden utilizar como grupos de clientes definidos por el usuario. Sin embargo, se pueden modificar solamente sus nombres y las descripciones.

Visualización de grupos de clientes

Puede ver información de grupos de clientes para mostrar miembros de grupo.

Nota: Esta opción está disponible solamente si el multicliente está instalado (en modo activo o de instalación).

Procedimiento para ver la lista de grupo de clientes

1. En la ficha Administración, seleccione Gestión de seguridad y de roles.

2. Haga clic en Grupos de clientes.
Aparecerá la Lista de grupos de clientes.
Nota: Puede optar por ver u ocultar grupos de clientes mantenidos por el sistema.
3. (Opcional) Seleccione un grupo de cliente de la lista.
Aparecerá la información del grupo de clientes.
4. Modifique el grupo de clientes si es necesario.

Creación de grupos de clientes

Puede utilizar el producto para crear un grupo de clientes.

Procedimiento para crear un grupo de clientes

1. En la ficha Administración, seleccione Gestión de seguridad y de roles.
2. Haga clic en Grupos de clientes.
Aparecerá la Lista de grupos de clientes.
Nota: La opción Gestión de seguridad y de roles, Grupos de clientes está disponible solamente cuando la función multicliente está instalada (ya sea activada o configurada).

3. Haga clic en Crear nuevo.
Aparecerá la página Crear nuevo grupo de clientes.
4. Rellene los siguientes campos:

Nombre de grupo de clientes

Muestra el nombre del grupo de clientes seleccionado.

Estado de registro

Establece el grupo de clientes como activo o inactivo.

Descripción

Muestra una descripción del grupo de clientes.

5. Haga clic en Guardar.
Se crea el grupo de clientes.
6. Cierre la ventana.
Aparecerá la Lista de grupos de clientes.

7. Haga clic con el botón secundario en la lista de clientes y seleccione Actualizar.
La Lista de grupos de clientes se actualiza.
8. Haga clic en Actualizar clientes en la página Detalles de grupo de clientes para agregar miembros de cliente al grupo.

Edición de grupos de clientes

Puede editar un grupo de clientes para gestionar sus miembros e información detallada.

Nota: Esta opción está disponible solamente si el multicliente está instalado (en modo activo o de instalación).

Procedimiento para editar un grupo de clientes

1. En la ficha Administración, seleccione Gestión de seguridad y de roles.
2. Haga clic en Grupos de clientes.
Aparecerá la Lista de grupos de clientes.
3. Haga clic con el botón secundario en un grupo de clientes y, a continuación, en Editar.
Aparecerá la página Actualizar grupo de clientes.
4. Realice las modificaciones adecuadas y haga clic en Guardar.
5. Cierre la ventana.
Aparecerá la Lista de grupos de clientes.
6. Haga clic con el botón secundario en la ventana y seleccione Actualizar.
Aparecerá la Lista de grupos de clientes actualizada.

Asignaciones de datos de cliente

CA Service Desk Manager muestra el cliente en el mismo formato en las versiones de Vista y Editar de una página de detalles para un objeto existente, porque el cliente para un objeto existente no puede ser cambiado de la interfaz Web.

Cuando edita un objeto de cliente, las listas desplegables de la página de edición se restringen automáticamente a los valores que son públicos, de propiedad del mismo cliente que el objeto base o cualquier cliente superior en la jerarquía de clientes, o de propiedad del proveedor de servicios (si la lista desplegable se aplica a un atributo SERVICE_PROVIDER_ELIGIBLE).

No hay cambios en la página de detalles para los campos de búsqueda asociados con un objeto de cliente. Si un usuario con acceso a varios clientes hace clic en un vínculo de búsqueda a una tabla de cliente, el motor Web restringe automáticamente la búsqueda a los valores apropiados para el atributo y muestra un mensaje banner en la búsqueda emergente o en la página de lista.

Nota: Las restricciones de cliente no se muestran en el filtro de búsqueda, y no pueden ser cambiados por el usuario.

El cliente se convierte en un selector (o una búsqueda o una lista desplegable) cuando solicita crear un objeto necesario de cliente.

Si el campo de cliente está vacío, puede especificar un valor de cliente directamente completando el campo, o indirectamente especificando un valor para un atributo que implica el cliente (como Usuario final afectado). La interfaz muestra los sufijos siguientes:

(T)

Indica un atributo que implica el cliente; es decir, una búsqueda a una tabla opcional de cliente.

(TO)

Indica un atributo que implica el cliente opcionalmente; es decir, una búsqueda a una tabla necesaria de cliente.

Las propiedades web.cfg controlan el texto de estos indicadores.

Excepto el atributo de cliente mismo, los atributos que implican el cliente siempre se muestran como búsquedas, aún si fueron creados con una macro de dtlDropdown.

CA Service Desk Manager automáticamente establece el cliente cuando busca o rellena automáticamente un valor de cliente en cualquier campo que implica el cliente (excepto que rellenar un campo SERVICE_PROVIDER_ELIGIBLE con una referencia a un objeto de proveedor de servicios no establezca el cliente). Una vez que el cliente está establecido, las búsquedas de campos que impliquen el cliente se restringen de la misma manera que las de los objetos de cliente existentes.

Nota: Hasta que guarda el objeto, el campo de cliente permanece editable, y puede cambiar el cliente directamente actualizándolo. Cuando cambia el cliente, CA Service Desk Manager automáticamente borra algunos campos que implican el cliente, y que contienen referencias a objetos que le pertenecen al cliente anterior.

CA Service Desk Manager inicializa normalmente el selector Cliente como vacío. Puede cambiar este comportamiento de varias maneras:

- Abra la página Crear nuevo desde una página como Perfil rápido, que rellena un campo que implica el cliente
- Establezca las preferencias de usuario Retener cliente
Ésta es una nueva preferencia de usuario que inicializa al cliente para objetos nuevos para el mismo cliente como la última página de detalles vista o actualizada, o en la última restricción de filtro de búsqueda de página de lista.
- Abra la página con una URL que especifique explícitamente a un cliente
Esto no se proporciona en ninguna URL predefinida, pero está disponible para permitir que los sitios creen elementos de menú o botones que especifican a un cliente.

Nota: Si crea elementos de configuración desde otro producto de CA (como CA APM) o desde la interfaz de línea de comandos, entonces el objeto es público.

Más información:

[Creación de un nuevo objeto de cliente](#) (en la página 90)

Creación de un nuevo objeto de cliente

El proveedor de servicios puede agregar datos específicos de cliente a objetos como incidencias, solicitudes, órdenes de cambio, etc. Puede agregar un cliente a un ticket (como un incidente) que se crea en una ficha Panel de resultados.

Procedimiento para agregar datos de cliente a un incidente

1. Haga clic en Archivo, Nuevo incidente.
2. Realice cualquiera de los pasos siguientes:
 - a. Seleccione el cliente de la lista desplegable Cliente.
 - b. Haga clic en Usuario final afectado (o cualquier otro campo que implica de cliente).
Aparecerá la página Búsqueda de contactos. Busque un usuario; puede filtrar la búsqueda por cliente.
 - c. Introduzca un nombre en el campo Usuario final afectado.
Los datos de cliente se completan automáticamente.
3. Continúe con la creación del incidente.

Notificaciones de actividades

Las notificaciones de actividades controlan el contenido de las notificaciones y los contactos que reciben notificaciones para diversos eventos en el historial de un ticket.

En un entorno de multicliente, la regla de notificación es un objeto opcional de cliente. Las reglas de notificación públicas se aplican a todos los tickets; las reglas de cliente se aplican solamente a tickets con el mismo cliente que la regla, o a los clientes de su jerarquía de subcliente. La restricción de clientes se aplica además de cualquier condición especificada en la regla misma.

Más información:

[Copia de las reglas de notificación](#) (en la página 91)

Copia de las reglas de notificación

Las reglas de notificación predeterminadas se almacenan como objetos públicos. Si se instala el multicliente, debe crear una copia de la regla de notificación para cada uno de los clientes, de lo contrario, se restringe la opción Actualizar contactos.

Procedimiento para copiar una regla de notificación

1. Navegue a Notificaciones, Reglas de notificación en la ficha Administración.
Aparece la Lista de reglas de notificación.
2. Haga clic en una regla de la columna Símbolo.
Aparecerá la página Detalles de regla de notificación.
3. Haga clic en Archivo, Copiar.
Reanude la actualización de la regla de notificación.

Repositorios

El objeto de repositorio (doc_rep) es opcional de cliente. Los clientes pueden definir sus propios repositorios y es posible definir repositorios públicos para objetos como datos adjuntos a documentos de conocimiento públicos. Cada cliente puede tener su propio repositorio predeterminado, y usted puede especificar un repositorio público predeterminado.

Todos los datos adjuntos son públicos o están asociados con un sólo cliente. Si un cliente no tiene su propio repositorio predeterminado, el repositorio público se muestra como el predeterminado para sus objetos de cliente.

Capítulo 4: Implementación de pólizas

Esta sección contiene los siguientes temas:

[Implementación de pólizas](#) (en la página 93)

[Notificaciones](#) (en la página 93)

[Administración de correo electrónico](#) (en la página 133)

[Acuerdos de nivel de servicio](#) (en la página 157)

[Seguridad](#) (en la página 171)

[Autenticación de usuarios](#) (en la página 183)

[Registros internos](#) (en la página 186)

[Integración de CA Service Desk Manager](#) (en la página 187)

[Asociaciones de partición de datos](#) (en la página 187)

[Encuestas](#) (en la página 194)

[Servicios Web](#) (en la página 197)

Implementación de pólizas

Una clave para configurara el centro de servicio al usuario consiste en implementar pólizas del modo que mejor se ajuste a sus procesos de negocio.

CA Service Desk Manager proporciona una implementación de política predefinida que es apropiada para algunos sitios y sirve como buen punto de partida para otros. Revise la implementación predeterminada en todas las áreas de definición de pólizas para determinar qué partes podrían cubrir sus necesidades y qué partes necesita modificar.

Notificaciones

CA Service Desk Manager permite notificar de forma automática al personal clave sobre las actividades de tickets (investigación, escalación, etc.) y los eventos (apertura de tickets, por ejemplo). Puede notificar también al personal clave sobre la tarjeta de informes de conocimiento (KRC) y las sesiones de asistencia de Automatización de soporte. Cuando se produce alguna actividad o evento de importancia, CA Service Desk Manager crea un mensaje de notificación donde se registra lo siguiente:

- Se identifica la actividad de parte o el evento notificado.
- Se hace referencia al parte.

- Se incluye otra información.
- Si se desea, se identifican los posibles contactos.

Puede ver un mensaje de notificación de un ticket a causa de una acción del sistema. Una acción del sistema incluye abrir, cerrar o modificar un ticket a través de su información de historial.

Establecer notificaciones automáticas implica las siguientes tareas:

- Definir notificaciones de actividades que determinan los tipos de actividades que generan notificaciones.
- Definir las notificaciones a contactos de objetos que determinan los contactos de objetos que se pueden utilizar para enviar notificaciones de actividades.
- Identificación de los métodos utilizados para enviar los mensajes.

Asociaciones de actividades

Puede definir tipos de actividad que se pueden asociar a un atributo de un objeto. Las asociaciones de actividades le permiten hacer lo siguiente:

- Seguir e informar los cambios a un atributo de objeto.
- Marcar una asociación de actividades como interna.

Las asociaciones de actividades internas limitan las notificaciones a los contactos cuyo tipo de acceso les permite ver registros internos. De este modo, los contactos que no tengan autorización para ver registros internos no reciben ninguna notificación aunque estén incluidos como destinatarios. Todos los registros de actividades futuros creados con la actividad asociada se marcan como internos.

Nota: Cada atributo de objeto puede tener solamente una asociación de actividad.

Notificaciones de actividades

Una actividad es una acción que alguien realiza, como resolver un ticket, enviar una encuesta gestionada, ejecutar la tarjeta de informes de conocimiento, etc. Las notificaciones de actividades identifican los tipos de actividades que provocan la notificación automática en el caso de los partes. Puede definir una notificación que se envía para una actividad específica. Por ejemplo, puede enviar una notificación por correo electrónico a un usuario afectado para obtener más información. El usuario puede responder al correo electrónico con la información solicitada a través de un dispositivo como un PDA. Incluso actividades diarias tales como devolver una llamada, cancelar o cerrar un registro, aumentar la prioridad o actualizar el estado pueden provocar el envío de una notificación.

Por lo general, las notificaciones de actividad implican el inicio o la finalización de acciones acerca de las cuales desea informar a determinados miembros del personal, por ejemplo, cuando se escalan tickets, cuando se transfieren o cuando se controlan. Cada vez que tiene lugar una actividad de ticket, CA Service Desk Manager comprueba si está seleccionada la notificación automática para dicha actividad. En caso afirmativo, la notificación de la actividad define qué mensaje se debe enviar al proceso de notificación.

También puede realizar las siguientes acciones en una notificación de actividad:

- Crear una regla de notificación que defina las directrices para que el sistema las siga al enviar notificaciones. Por ejemplo, establezca una notificación de actividad que notifica al asignatario anterior (o grupo) cuando cambia algo en un ticket.
- Establecer una notificación de actividad manual que actualiza un ticket cuando el usuario responde.

Nota: No puede mantener diferentes notificaciones de actividad manuales por cliente ni copiar una notificación de actividad manual.

- Adjuntar eventos.

Más información:

[Registros internos](#) (en la página 186)

[Reglas de notificación](#) (en la página 105)

[Notificaciones de asignatario anteriores](#) (en la página 123)

[Notificaciones de elementos de configuración](#) (en la página 34)

[Cómo funcionan las notificaciones de actividades](#) (en la página 96)

Cómo funcionan las notificaciones de actividades

Puede definir una notificación que se envía para una actividad específica. Se pueden definir notificaciones de actividades para solicitudes, incidentes, problemas, órdenes de cambio, incidencias, encuestas gestionadas, documentos de conocimiento, comentarios de documento de conocimiento, tarjetas de informes de conocimiento, sesión de asistencia, contactos y elementos de configuración.

Al definir una notificación de actividad, se puede configurar lo siguiente:

Eventos

Define la lista de eventos para esta notificación de actividad. Los eventos son procedimientos que el sistema de gestión de incidencias sigue cuando transcurre un tiempo determinado.

Reglas de notificación

Define nuevas reglas de notificación para solicitudes/incidentes/problemas, órdenes de cambio, incidencias. También puede modificar las reglas predeterminadas que aparecen en la lista Reglas de notificación.

Estudio

Define una notificación de encuesta que permite al destinatario de esta notificación de actividad hacer clic en una URL para ver una encuesta. Las encuestas permiten recopilar y analizar la opinión de los clientes.

Nota: Para obtener más información sobre la creación de notificaciones de actividades para solicitudes, órdenes de cambio, incidencias, encuestas gestionadas, documentos de conocimiento, comentarios de documento de conocimiento, tarjeta de informes de conocimiento, sesión de asistencia, contactos o elementos de configuración, consulte la *Ayuda en línea*.

Notificaciones a contactos de objetos

Las notificaciones de contactos de objetos permiten notificar a los destinatarios basándose en el valor actual de un campo en el ticket. En lugar de identificar a una persona a la que desea notificar, como en un método de notificación, identifica un objeto. Por ejemplo, puede identificar el campo Para de forma que se asegure de que esa notificación va a la persona actualmente identificada en el campo Para, aunque el valor haya cambiado desde que se definió el ticket.

Procedimiento para crear una notificación de contacto de objeto

1. En la ficha Administración, vaya a Notificaciones, Notificaciones de contacto del objeto.

Aparecerá la página Lista de notificaciones a contactos de objetos.

2. Haga clic en Crear nuevo.

Se abrirá la página Crear nueva notificación de contacto de objeto.

3. Rellene los siguientes campos:

Símbolo

Define un identificador exclusivo de la notificación de contacto de objeto.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Especifica si la notificación de contacto de objeto está activa o inactiva.

Tipo de objeto

Muestra el nombre del objeto al que se aplican los atributos.

Nombre de atributo de objeto

Ofrece el nombre de la notificación de contacto de objeto (en el campo Símbolo) en Majic, que es el código interno de Computer Associates. El nombre de atributo depende de la selección del tipo de objeto:

- Si el tipo de objeto es Incidencia o Tarea de workflow, el nombre de atributo es asignatario, solicitante o grupo; éstos son los nombres de atributo en los objetos chg y se asignan a los campos de las tablas Change_Request.
- Si el tipo de objeto es un registro de actividades de incidencia, el nombre del atributo tiene que empezar por el nombre de atributo del objeto del registro de actividades que lo vincula a una creación de instancia específica del objeto chg. El nombre de atributo podría ser change_id.group.

Descripción

Describe la notificación de contacto de objeto.

4. Haga clic en Guardar.

El método de notificación de contacto de objeto nuevo aparecerá en la lista de notificaciones de contacto de objeto cuando se vuelva a mostrar la lista.

Métodos de notificación

Los métodos de notificación describen cómo se entregan los mensajes de notificación a los usuarios. Los métodos de notificación son secuencias de comandos que se invocan en función de notificaciones de actividad. Las secuencias de comandos utilizan la información suministrada como variables para notificar al personal u otros sistemas de algo que ha ocurrido. Por ejemplo, se puede escribir una secuencia de comandos que sirva para enviar un correo de voz al analista asignado a una solicitud con el fin de avisarle de que se ha escalado dicha solicitud.

Se pueden asignar métodos de notificación para cada registro de contacto. El sistema busca el método de notificación que se debe utilizar para determinados contactos.

Los métodos de notificación estándar de CA Service Desk Manager son los siguientes:

- La función de correo electrónico envía mensajes por este medio directamente al destinatario mediante el protocolo simple de transferencia de correo (SMTP). Los mensajes también se envían al registro de notificaciones del destinatario.
- La función de notificación envía mensajes al registro de notificaciones del destinatario que es accesible para éste cuando se está ejecutando CA Service Desk Manager.
- La función de correo electrónico de localizador envía mensajes de correo electrónico a direcciones de cuyo mantenimiento se ocupa un proveedor de sistemas de localización. El texto del mensaje se suele mostrar en un localizador alfanumérico.

También puede crear sus propios métodos de notificación. Por ejemplo, se puede enviar una notificación a una impresora determinada para la recopilación periódica o a un buscapersonas. Para crear un método de notificación, cree un script de shell que incluya variables de notificación y, a continuación, introducir el nuevo método en CA Service Desk Manager.

Nota: Para obtener más información sobre los métodos de notificación, consulte la *Guía de implementación*.

Más información:

[Configuración de notificaciones según el tipo de contacto](#) (en la página 202)

pdm_mail Utility: enviar información por correo electrónico

La utilidad `pdm_mail` se utiliza en notificaciones para enviar correos electrónicos mediante el envío de información por correo electrónico al proceso `pdm_mail_nxd`. La utilidad `pdm_mail` se puede utilizar también para comandos, pero no para ambos. Si ningún parámetro se utiliza, entonces el comportamiento predeterminado de utilizar la variable `NX_NTF_xxxx` para pasar parámetros entra en efecto.

Para el correo electrónico, la utilidad se invoca de la siguiente manera:

```
pdm_mail [-i [-s subject] [-e email_address] [-q]] [-p] [-M] [-F] [-T] [-B] [-H]
[-N] [-R] [-h]
```

-i

Usa STDIN en lugar de variables de NTF. Los parámetros siguientes se utilizan para el comportamiento de correo electrónico de STDIN solamente:

-e

Especifica la dirección de correo electrónico (por destinatario).

-s

Especifica el asunto del mensaje de correo.

-q

Deshabilita la solicitud de STDIN.

-p

Utiliza la lógica de buscapersonas. Esta opción incluye el uso de la dirección de correo electrónico de buscapersonas en lugar de la dirección de correo electrónico regular. Solamente la versión de texto sin formato de la notificación se utiliza (HTML).

-M

Usa texto sin formato solamente (no MIME) en el cuerpo.

-F

Especifica la dirección Desde del correo electrónico.

-T

Especifica la dirección Responder a del correo electrónico.

-B

Especifica la codificación de caracteres del cuerpo. Esto puede ser útil para buscapersonas que no admiten UTF-8.

-H

Especifica la codificación de caracteres del encabezamiento. Esto puede ser útil para buscar personas que no admiten UTF-8.

-N

Especifica la opción de notificación Notificación de estado del envío (DSN).

-R

Especifica la opción de devolución Notificación de estado del envío (DSN).

-h

Muestra la ayuda en la utilidad.

Para los comandos, la utilidad se invoca de la siguiente manera:

Comando para el servidor de correo

```
pdm_mail -c option [parámetro]
```

Comando para maileater

```
pdm_mail -x option [parámetro]
```

check_interval

(-x solamente) Cambia el intervalo de comprobación de correos a un valor especificado (en segundos).

report_interval

Cambia el intervalo de informe a un valor especificado (en segundos).

report_now

Fuerza un informe de los registros. El contador no se restablece.

send_q

(-c solamente) Envía la cola de correo local al servidor de correo remoto.

trace

Activa o desactiva el seguimiento.

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

Notificaciones por correo electrónico

Las notificaciones por correo ayudan a los analistas a comunicarse con empleados y usuarios finales.

Los empleados y los usuarios finales dentro de un entorno son a veces móviles e interactúan con CA Service Desk Manager mediante el correo electrónico. Puede configurar CA Service Desk Manager para que este tipo de usuario pueda hacer lo siguiente:

- Actualizar una orden de cambio/problema/incidente/petición por medio de una respuesta a una notificación por correo electrónico enviada desde CA Service Desk Manager.
- Aceptar o rechazar una tarea de workflow (clásico o CA Workflow) mediante el correo electrónico.

Las notificaciones permiten comunicarse con los interesados para un ticket de la siguiente manera:

- Las notificaciones por correo electrónico pueden mostrar todos los destinatarios de la notificación, y aconsejar al usuario sobre quiénes son las partes interesadas.
- Los analistas pueden enviar una notificación manual a una dirección de correo electrónico temporal que no está asociada actualmente a un contacto. Una dirección temporal es útil, por ejemplo, cuando un usuario final se encuentra fuera de la oficina o tiene dificultades para acceder a su cuenta de correo electrónico estándar.
- Los analistas pueden enviar adjuntos con una notificación para comunicar detalles adicionales a un usuario.

Direcciones de correo electrónico provisionales

Una dirección de correo electrónico temporal es una dirección que no se asocia con un contacto del sistema.

Las direcciones de correo electrónico temporales son útiles en circunstancias como las siguientes:

1. Un usuario final está fuera de la oficina o está teniendo dificultades para acceder a su cuenta de correo electrónico estándar.
2. El analista quiere utilizar el correo electrónico para realizar un seguimiento de las interacciones con el usuario.

3. El analista envía una notificación manual a una dirección de correo electrónico *temporal* para el usuario.
4. El analista puede ver el registro de actividades, que se actualiza con la notificación manual.

Nota: Si desea obtener información sobre la configuración de las direcciones de correo electrónico temporales, consulte la *Ayuda en línea*.

Permitir direcciones de correo electrónico provisionales

Puede permitir que los usuarios envíen notificaciones manuales a direcciones de correo electrónico provisionales. Por ejemplo, los analistas pueden enviar correo electrónico a una dirección que no se asocia con un registro de contacto. Los destinatarios no pueden responder a direcciones provisionales cuando sus direcciones de correo electrónico no se asocian con un registro de contacto o no tienen permiso para actualizar el ticket.

Nota: Las direcciones de correo electrónico provisionales son siempre direcciones de correo electrónico SMTP y se admiten solamente cuando el método preferido es compatible con SMTP.

Para permitir direcciones de correo electrónico provisionales

1. En la ficha Administración, vaya a Gestor de opciones, Notificaciones.
Aparecerá la Lista de opciones.
2. Haga clic en `notification_allow_temp_address`.
Aparecerá la página Detalles de opciones de `notification_allow_temp_address` con los valores predeterminados establecidos.
3. Haga clic en Editar.
Aparecerá la página Actualización de opciones de `notification_allow_temp_address` con los valores predeterminados establecidos, y puede editar la descripción.
4. Haga clic en Instalar.
Aparecerá la página Detalles de opciones de `notification_allow_temp_address`.
5. Haga clic en Cerrar ventana.
6. Reinicie el servidor de CA Service Desk Manager.
Ahora se permiten las direcciones de correo electrónico temporales para las notificaciones manuales.

No permitir direcciones de correo electrónico provisionales

De manera predeterminada, los usuarios no pueden enviar notificaciones de actividad manuales a direcciones de correo electrónico temporales. Por ejemplo, los analistas no pueden enviar correo electrónico a una dirección que no esté asociada con un registro de contacto. Los administradores instalan la opción `notification_allow_temp_address` para permitir direcciones de correo electrónico temporales. Si la opción se instala y no quiere permitir notificaciones manuales a direcciones de correo electrónico temporales, puede desinstalar la opción.

Nota: Las direcciones de correo electrónico temporales utilizan direcciones de correo electrónico SMTP y el método de notificación Método preferido.

Para no permitir direcciones de correo electrónico temporales

1. En la ficha Administración, vaya a Gestor de opciones, Notificaciones.
Aparecerá la Lista de opciones.
2. Haga clic en `notification_allow_temp_address`.
Aparecerá la página Detalles de opciones de `notification_allow_temp_address`.
3. Haga clic en Editar.
Aparecerá la página Actualizar opciones de `notification_allow_temp_address`.
4. Haga clic en Desinstalar.
Aparecerá la página Detalles de opciones de `notification_allow_temp_address`.
5. Haga clic en Cerrar ventana.
6. Reinicie el servidor de CA Service Desk Manager.
La opción se desinstala y las direcciones de correo electrónico temporales no se permiten ahora para las notificaciones de actividad manuales.

Sondeo de buzón de correo

Si se produce un error en el servidor de correo saliente, no se enviarán las notificaciones de correo electrónico ni se pondrán en cola en el directorio `%NX_ROOT%\site\mail_queue`. Cuando el servidor de correo se vuelve activo otra vez, después de un intervalo, procesa y envía el correo electrónico. Puede cambiar el intervalo para reciclar el correo electrónico que se puso en cola cuando el servidor de correo estaba ocupado.

Los mensajes de correo electrónico de notificación que el servidor de correo saliente no puede enviar se reenvían hasta que realice una de las siguientes acciones:

- Detener el daemon de correo (pdm_mail_nxd) que trata las notificaciones de correo electrónico saliente.
- Suprimir manualmente los mensajes del directorio
%NX_ROOT%\site\mail_queue.

Cómo establecer la variable de intervalo de reintentos de correo electrónico

Puede definir el intervalo de tiempo (en segundos) a fin de reintentar intentos fallidos de enviar correo electrónico saliente al servidor de correo.

Nota: CA Service Desk Manager no reintenta enviar los mensajes que el servidor de correo saliente acepta, pero que no se pueden entregar. En el caso de estos mensajes, se aplican las políticas y características de reintento del servidor de correo saliente, si las hubiese.

Los reintentos se llevan a cabo por mensaje. Si el servidor de correo no está disponible durante un período, se vuelve a intentar cada mensaje cuando caduca su propio temporizador, en lugar de enviar todos los mensajes a la vez. Sin embargo, si reinicia el daemon de correo saliente, todos los mensajes no enviados intentan enviarse en ese momento y, si se produce un error en el envío, todos sus temporizadores de reintento se restablecen al mismo tiempo.

El valor (NX_EMAIL_RETRY_INTERVAL) en el archivo NX.env controla el intervalo de reintentos. Puede cambiar el valor predeterminado del intervalo de reintentos en uno o más servidores.

Procedimiento para establecer el intervalo de reintentos de correo electrónico

1. Desplácese al directorio \$NX_ROOT en el servidor.
2. Utilice un editor de texto como WordPad para abrir el archivo NX.env.
3. Modifique el valor en el intervalo NX_EMAIL_RETRY_INTERVAL que desee de la siguiente forma:

```
NX_EMAIL_RETRY_INTERVAL=number_of_seconds
```

NX_EMAIL_RETRY_INTERVAL

Define el intervalo de tiempo (en segundos) para reintentar intentos fallidos de correo electrónico.

number_of_seconds

Especifica el número de segundos para cada intervalo de reintentos de correo electrónico. El tiempo predeterminado es 600 segundos (10 minutos). El valor mínimo que puede utilizar es 20 segundos. Si establece un valor inferior al mínimo de 20 segundos o superior al máximo de 2000000 de segundos, se utiliza el valor predeterminado de 10 minutos.

4. Guarde y cierre el archivo.
5. Reinicie el servicio de CA Service Desk Manager.

El cambio surte efecto.

Reglas de notificación

Una regla de notificación permite definir directrices para que el sistema las siga al enviar las notificaciones. Mediante las reglas de notificación, puede especificar a quién se notifica automáticamente y en qué circunstancias.

Puede definir reglas de notificación para solicitudes, incidentes, problemas, órdenes de cambio, incidencias, contactos, elementos de configuración y clientes globales y específicos. Cada regla de notificación contiene los siguientes componentes:

Macro de condición

Configúrela para representar los valores deseados de uno o más campos de un ticket del centro de servicio al usuario. La condición se evalúa en puntos diferentes durante el proceso para determinar si ocurre una acción.

Plantilla de mensajes

Contiene un prototipo del mensaje que se genera y se envía a los contactos cuando se envía la notificación. Una regla de notificación debe contener una plantilla de mensaje y se pueden volver a utilizar.

Contactos de objeto

Muestra el contacto de objeto derivado de la información del ticket, como asignatario, usuario final, grupo, etc. Si se cumple la condición, estos contactos de objeto reciben la notificación.

Contactos

Si se cumple la condición, estos contactos reciben la notificación. Los contactos son los registros de la base de datos que representan a los usuarios del sistema.

Tipos de contactos

Muestra el tipo de contacto del que quiere recibir la notificación de forma predeterminada, por ejemplo, Analistas, Empleado, Cliente, etc.

Notificaciones de actividades relacionadas

Muestra una lista de notificaciones de actividades relacionadas que utilizan la regla de notificación.

Nota: Los usuarios pueden recibir varias notificaciones para una notificación de actividad que contenga varias reglas para las que estos cumplen las condiciones.

Opciones de configuración de las reglas de notificación

Puede especificar las siguientes opciones cuando define una regla de notificación:

- **Regla de notificación predeterminada:** puede especificar una regla de notificación predeterminada que automáticamente notifica a todos los contactos identificados en el campo al cual se hace referencia en el ticket. Para ver la lista de reglas de notificación predeterminadas que puede modificar, seleccione la ficha Administración, Notificaciones, Reglas de notificación.
- **Macro de condición definida por el sitio:** puede implementar una *macro de condición definida por el sitio* para crear su propia condición que solamente notifica a contactos específicos en ciertas circunstancias. Para crear una macro de condición desde la ficha Administración, seleccione Eventos y macros, Tipos de macros, y luego Condición definida por el sitio en la lista Tipo de macros.
- **Nuevos contactos:** cuando define una regla de notificación, puede identificar nuevos contactos para recibir notificaciones en las siguientes fichas:
 - **Contactos de objeto:** muestra las organizaciones, los proveedores y los elementos de configuración disponibles para el tipo de objeto seleccionado que recibirá la notificación acerca de los tickets.
 - **Contactos:** muestra los individuos que se han agregado a la regla de notificación, independientemente de su afiliación con el ticket.
 - **Tipos de contacto:** muestra los usuarios que se han definido en la regla de notificación con la misma clasificación, como analista o cliente.

El botón Actualizar de cada ficha le permite buscar nuevos registros de contacto para asociar con la regla.

Nota: Antes de implementar una regla de notificación, configure los contactos apropiados para su estructura de negocio.

- **Plantilla de mensaje:** todas las reglas de notificación deben contener una plantilla de mensaje. Puede definir su propia plantilla de mensaje o especificar una de las plantillas de mensaje predeterminadas disponibles en la página Lista de plantillas de mensaje. Para ver esta página, seleccione la ficha Administración, Notificaciones, Plantillas de mensaje.

- **Notificaciones de elemento de configuración:** cuando define una regla de notificación, puede identificar a la persona responsable de mantener un elemento de configuración para que reciba notificaciones cuando se crea un ticket.
- **Notificaciones de asignatario anterior:** cuando define una notificación de actividad, puede especificar valores en la regla de notificación para que se notifique al asignatario o grupo anteriores cuando ocurre una actividad de evento.

Más información:

[Cómo definir la estructura de negocio](#) (en la página 45)

[Ejemplo: creación de una plantilla de mensajes](#) (en la página 116)

[Notificaciones de asignatario anteriores](#) (en la página 123)

[Notificaciones a contactos de objetos](#) (en la página 96)

[Descripción general de la macro de condición definida por el sitio](#) (en la página 107)

Descripción general de la macro de condición definida por el sitio

Un gestor desea recibir información sobre todas las actividades de ticket llevadas a cabo para las incidencias de prioridad 2 correspondientes a su departamento. El administrador agrega al gestor como contacto específico en determinados tipos de notificaciones de actividades, como Inicial y Comentario de registro. Con esta implementación, el gestor recibe todas las notificaciones de actividades seleccionadas para todo el sistema.

En un departamento de gran volumen, como Soporte técnico, el tráfico de correo electrónico no deseado puede ser significativo. Para controlar el buzón de correo, el gestor debe implementar reglas de buzón de correo con el fin de filtrar las notificaciones y asegurarse de no perder información importante.

El administrador define una macro de condición definida por el sitio según la cual sólo notifica al gestor cuando el campo Prioridad se establece en 2 y el Área de solicitud se establece en Aplicaciones (departamento del gestor). La nueva condición se especifica en la regla de notificación y el gestor se agrega como contacto. Se define una plantilla de mensaje que describe la actividad del ticket y la regla se agrega a la notificación de actividades.

La actividad se desarrolla cuando la prioridad de un ticket se establece en 2 y el área de solicitud se establece en Aplicaciones. Cuando esta actividad se lleva a cabo, se implementa la regla y se evalúa la condición. Si la condición se evalúa como Verdadera, se le envía al gestor un mensaje de notificación que describe la actividad del ticket. El gestor no recibe notificaciones no deseadas.

Regla de notificación de ejemplo

Los ejemplos de la regla de notificación ofrecen información introductoria que le ayudará a lograr lo siguiente:

- Procedimiento para crear una macro de condición definida por el sitio
- Procedimiento para crear una regla de notificación
- Cómo agregar la regla a la notificación de actividades

Cuando se produce la actividad, se implementa la condición correspondiente adjunta a la regla. Si se cumple la condición (se evalúa como *verdadera*), se envía un mensaje de notificación que describe la actividad del ticket a todos los contactos.

Más información:

[Ejemplo: creación de una macro de condición definida por el sitio](#) (en la página 108)

[Ejemplo: creación de una regla de notificación](#) (en la página 109)

[Ejemplo: cómo agregar reglas a la notificación de actividades](#) (en la página 110)

Ejemplo: creación de una macro de condición definida por el sitio

En este ejemplo, se crea una macro de condición definida por el sitio que comprueba la condición especificada.

1. En la ficha Administración, vaya a Eventos y macros, Macros.
Aparecerá la página Lista de macros.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nueva macro.
3. Rellene los siguientes campos:
 - Símbolo: introduzca *Aplicación P1*.
 - Tipo de macro: seleccione Condición definida por el sitio.
 - Tipo de objeto: seleccione Solicitud.
4. Haga clic en Continuar.
Aparecerá la página Crear nueva macro de aplicaciones P1.
5. Rellene los siguientes campos:
 - Descripción de la macro: escriba *Macro=Solicitud, Prioridad=1, Área de solicitud=Aplicaciones*.
 - Si todas las condiciones se cumplen, devolver: seleccione VERDADERA.
 - Estado del registro: seleccione Activo.

6. Haga clic en Guardar.
Aparecerá la página Detalles de macro de aplicaciones 1.
7. Haga clic en Agregar condición.
Aparecerá la página Crear nueva condición elemental.
8. Cree una condición elemental para comprobar la prioridad 2 y rellene los siguientes campos:
 - Secuencia: escriba *10*.
 - Descripción: escriba *Comprobar prioridad*.
 - Seleccionar un atributo: seleccione Prioridad.
 - Elegir operador: seleccione Igual.
 - Seleccionar un valor de datos o atributo: seleccione Valor de datos.
9. Seleccione 2 para el valor de datos y haga clic en Guardar.
10. En la página Detalles de macro, haga clic en Agregar condición y rellene los siguientes campos:
 - Secuencia: escriba *20*.
 - Descripción: escriba *Comprobar área de solicitud=Aplicaciones*.
 - Seleccionar un atributo: seleccione Área de solicitud.
 - Elegir operador: seleccione Igual.
 - Seleccionar un valor de datos o atributo: seleccione Valor de datos.
11. Seleccione Aplicaciones para el valor de datos y haga clic en Guardar.
Aparecerá la nueva condición en la ficha Condiciones de la macro de condición definida por el sitio.

Ejemplo: creación de una regla de notificación

En este ejemplo, se va a asociar la macro de condición definida por el sitio con la regla de notificación, se adjuntará una plantilla de mensajes y se agregará al gestor como tipo de contacto.

1. En la ficha Administración, vaya a Notificaciones, Reglas de notificación.
Aparecerá la página Lista de reglas de notificación.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nueva regla de notificación.

3. Rellene los siguientes campos:
 - Símbolo: escriba App1 notifica a gestores.
 - Tipo de objeto: seleccione Solicitud.
 - Descripción: escriba *Notificar a gestores sobre cortes en aplicación de prioridad 1*.
4. Haga clic en Guardar y continuar.
5. Haga clic en el vínculo Condición y seleccione la nueva macro de condición definida por el sitio denominada Aplicación P1.
6. Haga clic en Plantilla de mensajes.

Aparecerá la página Lista de plantilla de mensajes.
7. Seleccione una plantilla de mensaje de la lista. Asegúrese de que la opción Notificación automática esté activada en la plantilla de mensaje.
8. En la ficha Tipos de contacto, haga clic en el botón Actualizar tipo de contacto.

Aparecerá la página Búsqueda de tipos de contactos.
9. Haga clic en Buscar.

Aparecerá la lista Destinatarios de actualización de notificaciones.
10. Seleccione Gestor en la lista de la izquierda y haga clic en el botón de selección de contactos ($\geq$).
11. Cuando el contacto esté en la lista de la derecha, haga clic en Aceptar.
12. Guarde la regla de notificación.

La nueva regla de notificación aparecerá en la lista de reglas de notificación cuando se vuelva a mostrar la página.

Ejemplo: cómo agregar reglas a la notificación de actividades

En este ejemplo, el usuario activa la opción Notificación automática en la plantilla de mensajes y agrega la regla de notificación a la notificación de actividades.

1. En la ficha Administración, vaya a Notificaciones, Notificaciones de actividades.

Aparecerá la página Lista de notificaciones de actividades.
2. Seleccione la notificación de actividad inicial de la lista.

Aparecerá la página Detalles de notificaciones de actividades iniciales.
3. Verifique que el Tipo de objeto se establezca a Solicitudes, para que el bloc de notas aparezca en la información de configuración para solicitudes.

4. En la ficha Reglas de notificación, haga clic en Actualizar reglas de notificación.
Aparecerá la página Búsqueda de reglas de notificación.
5. Escriba *App1 notifica a gestores* en el campo Símbolo y haga clic en Buscar.
Aparecerá la página para actualizar las reglas de notificación asignadas.
6. Seleccione *App1 notifica a gestores* en la lista de la izquierda y haga clic en el botón de selección de contactos (>).
La regla de notificación está en la lista de la derecha.
7. Haga clic en OK.
8. Haga clic en el vínculo Condición y seleccione la nueva regla App1 notifica a gestores. (Puede agregar más reglas haciendo el botón Actualizar reglas de notificación).
Aparecerá la página Notificación de actividades.
9. Asegúrese de que la opción Notificación automática se establezca en la plantilla de mensaje de la siguiente manera:
 - a. Haga clic en el vínculo Regla de notificación en la ficha Reglas de notificación de la notificación de actividades.
Aparecerá la página Regla de notificación.
 - b. Haga clic en el vínculo Plantilla de mensaje.
Aparecerá la página Detalles de plantilla de mensaje.
 - c. Haga clic en Editar.
Aparecerá la página Actualizar plantilla de mensaje.
 - d. Verifique que Notificación automática esté habilitada.
10. Haga clic en Guardar.
Cuando se produce la actividad, se implementa la condición correspondiente adjunta a la regla. Si se cumple la condición (evalúa como verdadera), un mensaje de notificación que describe la actividad del ticket se les envía a todos los gestores.

Reglas de notificación predeterminadas de ejemplo

CA Service Desk Manager contiene varias reglas de notificación predeterminadas. Para ver las reglas de notificación predeterminadas, puede ir a Notificaciones, Reglas de notificación de la ficha Administración.

Más información:

[Ejemplo: utilización de la regla de solicitud de prioridad 1](#) (en la página 112)

[Ejemplo: utilización de la regla Notificar al asignatario actual y anterior de una orden de cambio](#) (en la página 113)

[Ejemplo: utilización de la regla Escalación de prioridad verdadera](#) (en la página 114)

[Ejemplo: utilización de la regla Activar solicitud/incidente/problema](#) (en la página 115)

Ejemplo: utilización de la regla de solicitud de prioridad 1

Las reglas de notificación proporcionan flexibilidad al usuario final cuando este desea recibir una notificación solamente para una solicitud de prioridad 1. La regla *Solicitud de prioridad 1* se ejecuta si el tipo de ticket es una solicitud y si la prioridad es 1. Esta notificación solamente se envía cuando la condición adjuntada a la regla se evalúa como verdadera y se utiliza la plantilla de mensaje asociada a la regla.

Nota: Para modificar la condición y la plantilla de mensaje de una regla de notificación, abra la regla y modifique el campo Condición con una macro. Para obtener más información sobre cómo modificar las condiciones, consulte la *ayuda en línea*.

El producto también incluye reglas de notificación predeterminadas denominadas "Incidente de prioridad 1" y "Problema de prioridad 1" que se determinan en la configuración de ITIL. La principal diferencia entre estas reglas y la solicitud de prioridad 1 son las condiciones para los tipos de ticket. Por ejemplo, la solicitud de prioridad 1 posee una condición con una secuencia "20" adjuntada a ella que limita la regla de notificación solamente a solicitudes.

De forma predeterminada, ningún contacto de objeto, contacto ni tipo de contacto está asociado a la regla. De forma predeterminada, el campo "Notificación automática" de la plantilla de mensaje adjuntada a la regla también se establece en la opción No. Para enviar una notificación, debe agregar un contacto de objeto, un contacto o un tipo de contacto a la regla y cambiar el campo Notificación automática de la plantilla de mensaje a la opción Sí.

Ejemplo: configuración de una regla de modo que sólo se envíe una notificación para las solicitudes cuya prioridad se ha establecido en 1

La regla debe conectarse a las notificaciones de actividades Inicial y Escalar. Esto permite garantizar que se reciba una notificación por una nueva solicitud de prioridad 1 y que se escale una solicitud a la prioridad 1.

1. Verifique que la regla predeterminada asociada a la notificación de actividades Inicial o Escalar se elimine o que la opción Notificación automática se establezca en No.

Esto impide que la notificación se envíe fuera de estas reglas predeterminadas.
2. Abra la regla Solicitud de prioridad 1.
3. Agregue un contacto de objeto, un contacto o un tipo de contacto a la regla.
4. Haga clic en Plantilla de mensaje y seleccione la opción Notificación automática.
5. Adjunte la regla Solicitud de prioridad 1 a las notificaciones de actividades Inicial y Escalar.
6. Realice los pasos siguientes:
 - Cree una nueva solicitud y establezca la prioridad en 1.
Verifique que el usuario reciba la notificación.
 - Cree una nueva solicitud y establezca la prioridad en un valor diferente como, por ejemplo, 2.
Verifique que el usuario no reciba la notificación.

Ejemplo: utilización de la regla Notificar al asignatario actual y anterior de una orden de cambio

La regla *Notificar el asignatario actual y anterior de una orden de cambio* notifica a ambos asignatarios, el actual y el anterior, de la orden de cambio durante una transferencia. También puede crear una regla similar para otros tipos de ticket.

Ejemplo: notificación al asignatario actual y anterior de una transferencia de orden de cambio

1. Verifique que la regla predeterminada adjuntada a la notificación de actividades Inicial se elimine o que la opción "Notificación automática" de la plantilla de mensaje adjuntada a la regla se establezca en No.

Esto impide que las notificaciones se envíen para estas reglas predeterminadas.
2. Abra la regla Notificar al asignatario actual y anterior de una orden de cambio.

3. Haga clic en la plantilla de mensaje "Notificar al asignatario actual y anterior de una orden de cambio" y seleccione la opción Notificación automática.
4. Adjunte la regla "Notificar al asignatario actual y anterior de una orden de cambio" a la notificación de actividades Transferencia.
5. Realice lo siguiente:
 - a. Cree y guarde una orden de cambio con un asignatario.
 - b. Realice la transferencia a un nuevo asignatario.Verifique que ambos usuarios reciban la notificación de transferencia.

Ejemplo: utilización de la regla Escalación de prioridad verdadera

La notificación de actividades denominada 'Escalar' se realiza cuando la prioridad de un ticket cambia, no sólo cuando la prioridad aumenta. Los usuarios reciben notificaciones tanto cuando la prioridad aumenta como cuando baja. Las reglas de notificación ahora proporcionan una forma de distinguir entre un cambio de la prioridad 2 a la prioridad 1 y un cambio de la prioridad 1 a la prioridad 2.

La regla *Escalación de prioridad verdadera* evalúa los valores actuales y anteriores del campo Prioridad. Esta regla envía una notificación al contacto del objeto, al contacto y a los tipos de contactos adjuntados a la regla solamente cuando la prioridad de un ticket de incidencia cambia de una prioridad menor a una mayor.

Nota: Puede crear una regla similar para otros tipos de ticket. Esta notificación solamente se envía cuando la condición adjuntada a la regla se evalúa como verdadera y se utiliza la plantilla de mensaje adjuntada a la regla. De forma predeterminada, ningún contacto de objeto, contacto ni tipo de contacto está adjuntado a la regla. De forma predeterminada, el campo Notificación automática de la plantilla de mensaje adjuntada a la regla también se establece en la opción No.

Ejemplo: recepción de una notificación cuando la prioridad cambia de una prioridad mayor a una menor en un tipo de ticket de incidencia

1. Verifique que la regla predeterminada adjuntada a la notificación de actividades Escalar se elimine o que la opción Notificación automática de la plantilla de mensaje adjuntada a la regla predeterminada se establezca en No.

Esto impide que las notificaciones se envíen fuera de estas reglas predeterminadas.

2. Abra la regla Escalación de prioridad verdadera.
Agregue un contacto de objeto, un contacto o un tipo de contacto a la regla.
Verifique que el contacto pueda recibir notificaciones.
3. Haga clic en Escalación de prioridad verdadera en el campo Plantilla de mensaje y seleccione la opción Notificación automática.
Adjunte la regla a la notificación de actividades Escalar.
4. Cree una nueva incidencia con una prioridad como, por ejemplo, 5.
5. Cambie la prioridad a 4 y verifique que el usuario reciba la notificación.
6. Cambie la prioridad de 4 a 5 y verifique que el usuario no reciba la notificación.

Ejemplo: utilización de la regla Activar solicitud/incidente/problema

La regla *Activar solicitud/incidente/problema* posee una condición adjuntada a ella para enviar la notificación inicial solamente cuando un elemento de solicitud/incidente/problema está activo.

Esto permite al cliente recibir la notificación de cierre sólo cuando se crea una solicitud inactiva. Esta regla envía una notificación al contacto del objeto, al contacto y a los tipos de contactos adjuntados a la regla solamente cuando se crea un elemento de solicitud/incidente/problema activo.

Nota: Puede crear una regla similar para los tipos de orden de cambio y ticket de incidencia.

Esta notificación se envía solamente cuando la condición adjuntada a la regla se evalúa como verdadera y se utiliza la plantilla de mensaje adjuntada a la regla. De forma predeterminada, ningún contacto de objeto, contacto ni tipo de contacto está asociado a la regla. De forma predeterminada, también el campo "Notificación automática" de la plantilla de mensaje adjuntada a la regla se establece en la opción No.

Ejemplo: recepción de una notificación cuando se cierra un incidente

1. Verifique que la regla predeterminada adjuntada a la notificación de actividades Inicial se elimine o que la opción "Notificación automática" de la plantilla de mensaje adjuntada a la regla predeterminada que a su vez está adjuntada a la notificación de actividades Escalar se establezca en No.
Esto impide que las notificaciones se envíen para estas reglas predeterminadas.

2. Abra la regla Activar solicitud/incidente/problema.
Agregue un contacto de objeto, un contacto o un tipo de contacto a la regla.
Verifique que el contacto pueda recibir la notificación.
3. Haga clic en la plantilla de mensaje "Activar solicitud/incidente/problema" adjuntada a la regla y seleccione la casilla de verificación "Notificación automática".
4. Adjunte la regla Activar solicitud/incidente/problema a la notificación de actividades inicial.
5. Cree un nuevo incidente y establezca el campo de estado en Cerrado.
6. Verifique que el usuario asignado que se ha configurado para recibir la notificación no reciba la notificación inicial.

Ejemplo: creación de una plantilla de mensajes

Todas las reglas de notificación deben contener una plantilla de mensaje. Puede crear plantillas que contengan valores predeterminados para utilizarlos en mensajes de notificación.

Ejemplo: creación de una plantilla de mensajes

En este ejemplo se explica cómo se crea una plantilla de mensajes.

Procedimiento para crear una plantilla de mensajes

1. En la ficha Administración, vaya a Notificaciones, Plantillas de mensajes.
Aparecerá la lista de plantillas de mensajes.
2. Haga clic en Crear nuevo.
Aparecerá la ventana Crear nueva plantilla de mensaje.
3. Rellene los siguientes campos:

Cliente

Especifica el cliente asociado a esta plantilla.

Nota: Si selecciona global (compartido) le permite utilizar la plantilla para mensajes globales.

Símbolo

Define un identificador exclusivo del registro.

Tipo de objeto

Especifica el tipo de objeto asociado con esta plantilla.

Estado de registro

Selecciona activo o inactivo para el estado de esta plantilla.

Notificación automática

Especifica que la notificación asociada a esta plantilla se enviará automáticamente cuando se produce la actividad.

Nivel de notificación

Indica la importancia relativa del envío de esta notificación. Seleccione Emergencia, Alto, Bajo o Normal.

Título del mensaje de notificación

Especifica el título de resumen del mensaje. Puede utilizar variables para insertar valores del ticket cuando se envíe una notificación. Por ejemplo, puede incluir una variable que inserta el número de incidencia en el título del mensaje.

Cuerpo del mensaje de notificación

Especifica el contenido del mensaje. Puede utilizar variables para insertar valores del ticket cuando se envíe una notificación. Por ejemplo, puede utilizar una variable que inserta el nombre del analista, el nombre del usuario final y la descripción en el mensaje.

Mensaje HTML

Especifica un mensaje en formato HTML que se debe mostrar si el programa de correo electrónico del destinatario admite mensajes HTML. Si el destinatario recibe el mensaje en un dispositivo de bolsillo, como un teléfono móvil o un Blackberry, el mensaje sólo se mostrará en texto sin formato.

Editar mensaje HTML

Abre el editor HTML, que permite editar el mensaje HTML.

Vista rápida

Muestra el mensaje tal y como le aparece al destinatario.

Código fuente HTML

Muestra el mensaje en código fuente HTML.

4. Haga clic en Guardar.

La plantilla de mensajes nueva aparecerá en la lista de plantillas de mensajes.

Artefactos en mensajes

Puede utilizar la palabra clave ARTEFACTO para especificar cómo se tratarán los artefactos en los mensajes salientes, plantillas de mensaje, notificaciones y respuesta automáticas. La palabra clave ARTEFACTO utiliza los siguientes valores:

- **NINGUNO:** no especifica ninguna validación de artefactos. Este valor equivale a no utilizar la palabra clave.
- **PROTEGIDO:** valida un ticket con respecto al hash para obtener confirmación. Si la confirmación falla, el artefacto se considera no válido y se produce un error en el filtrado al filtrar las búsquedas de un artefacto (`{{object_id}}`).
- **SEGURO:** descifra el número de ticket. Si el valor no es una contraseña válida, el artefacto se considera no válido y se produce un error en el filtrado al filtrar las búsquedas de un artefacto (`{{object_id}}`).

Frases y códigos de notificación

Las frases de notificación permiten agregar un texto o pieza de información normalizada a varios mensajes de notificación diferentes, sin tener que introducir y mantener por separado el texto o las fórmulas en cada plantilla de notificación. Por ejemplo:

Conteste esta notificación para agregar más información al ticket

Las frases normalizan texto para usarse en varias plantillas de mensaje. Por ejemplo, puede mantener una frase común como un aviso confidencial en un solo registro y utilizarla en varias plantillas de mensaje. Las frases de notificación también son útiles para respuestas de mensajes, como un aviso de respuesta o un vínculo Web de URL. CA Service Desk Manager proporciona frases, pero usted también puede crear sus propias frases. Puede establecer una frase como activa o inactiva para usarla globalmente en una plantilla de mensaje. (Las frases de notificación están inactivas de forma predeterminada). Cuando una frase está inactiva, ésta se suprime en todas las plantillas de mensaje que la utilizan.

Las frases de notificación también se pueden utilizar en las respuestas automáticas a mensajes de correo electrónico entrantes. El contexto de procesamiento para este tipo de mensaje es diferente; omita el prefijo (`change_id.`, `issue_id.`, `call_req_id.`) utilizado en ciertas macros como `ref_num` y `web_url` para las frases que el mensaje utiliza. Por lo tanto, no puede compartir frases de notificación entre plantillas de notificación y respuestas automáticas de correo electrónico.

Por ejemplo, éstas son algunas de las frases proporcionadas por CA Service Desk Manager:

Símbolo	Código	Frase
Historial de notificaciones: cambio	notify_history_chg	Haga clic en la URL siguiente para ver la Lista de notificaciones: @{change_id.web_url}+HTML=chg_lr.html+INSTANCE=@{id}
Historial de notificaciones: incidencia	notify_history_iss	Haga clic en la URL siguiente para ver la Lista de notificaciones: @{issue_id.web_url}+HTML=iss_lr.html+INSTANCE=@{id}
Historial de notificaciones: solicitud/incidente/problema	notify_history_cr	Haga clic en la URL siguiente para ver la Lista de notificaciones: @{call_req_id.web_url}+HTML=cr_lr.html+INSTANCE=@{id}

Ejemplo: nuevas frases

Las siguientes frases son ejemplos de frases que puede crear:

Símbolo	Código	Frase
Notificar confidencialidad	ConfidentialNotice	Este correo electrónico y los archivos que se transmiten con él son para el uso exclusivo de los destinatarios deseados y contienen información que puede ser privilegiada y confidencial. Quedan prohibidas la revisión, utilización, divulgación o distribución no autorizadas. Si usted no es el destinatario deseado de este correo electrónico, suprimalo junto con los archivos transmitidos y notifíquelo al remitente inmediatamente.
Notificar respuesta de incidente	IncidentReply	Para agregar un comentario al incidente, conteste este correo o incluya la línea siguiente (en una sola línea). %incident_id=@{call_req_id.ref_num}
Notificar URL de incidente	IncidentURL	Haga clic en la URL siguiente para ver: @{call_req_id.web_url}

Nota: Utilice frases independientes para las versiones HTML y en texto sin formato de las plantillas de mensaje o respuestas automáticas de correo electrónico. El HTML consolida casi todo el espacio en blanco en espacios únicos, de modo que los saltos de línea (o de párrafo) deben especificarse con etiquetas. Las etiquetas de HTML incluidas en las versiones de texto sin formato de los mensajes se muestran en lugar de procesarse.

Sintaxis de la frase de notificación

Puede insertar frases de notificación en plantillas de mensajes y mensajes de respuesta de correo electrónico que utilicen la siguiente sintaxis de macro:

```
@{notification_phrase[code].phrase}
```

código

Especifica el valor de código exclusivo, como ConfidentialNotice, de la tabla de frases de mensaje (usp_notification_phrase).

Nota: La tabla usp_notification_phrase enumera frases comunes que las plantillas de mensaje de notificación pueden utilizar. Para obtener más información sobre la tabla usp_notification_phrase, consulte la *Guía de referencia técnica*.

Por ejemplo:

```
@{notification_phrase[IncidentURL1].phrase}
```

```
@{notification_phrase[RequestReply].phrase}
```

Cuando CA Service Desk Manager localiza la macro, el texto de la frase de la tabla usp_notification_phrase reemplaza a la sintaxis. Si no existe ningún código que coincida (o si está inactivo), una cadena vacía reemplaza a la macro. No se escribe ningún error en el registro estándar (STDLOG); en cambio, se registra un mensaje de advertencia para ayudarle a resolver problemas potenciales.

Nota: La incrustación de mensajes dentro de otras frases se limita a un valor de profundidad máximo que se configura definiendo la variable de entorno (see page 356) NX_MAX_EXPAND_DEPTH. Esta limitación evita problemas que se pueden producir al procesar frases que accidentalmente se hacen referencia a sí mismas (se incrustan a sí mismas) o hacen referencia circular (cuando una frase incrusta una frase en la que está incrustada).

Cómo aparecen las frases de notificación en un ejemplo de mensaje

En este ejemplo se demuestra cómo aparecen las frases de notificación en un mensaje de notificación. El ejemplo utiliza los siguientes códigos y frases:

Código	Frase
ConfidentialNotice	Este correo electrónico y los archivos que se transmiten con él son para el uso exclusivo de los destinatarios deseados y contienen información que puede ser privilegiada y confidencial. Quedan prohibidas la revisión, utilización, divulgación o distribución no autorizadas. Si usted no es el destinatario deseado de este correo electrónico, suprimalo junto con los archivos transmitidos y notifíquelo al remitente inmediatamente.
IncidentReply	Para agregar un comentario al incidente, conteste este correo o incluya la línea siguiente (en una sola línea). %incident_id=@{call_req_id.ref_num}
IncidentURL	Haga clic en la URL siguiente para ver: @{call_req_id.web_url}

La siguiente plantilla de mensaje incluye las frases de notificación:

```
@{call_req_id.type.sym} @{call_req_id.ref_num} cerrado.
Asignado a: @{call_req_id.assignee.combo_name}
Cliente: @{call_req_id.customer.combo_name}
Descripción: @{call_req_id.description}

@{notification_phrase[IncidentURL].phrase}
@{notification_phrase[IncidentReply].phrase}

@{notification_phrase[ConfidentialNotice].phrase}
```

Las frases aparecen en los mensajes de la siguiente forma:

```
Incidente 1234 cerrado.
Asignado a: Analista, Pedro
Cliente: Pérez, Juan
Descripción: ésta es una descripción de mi problema

Haga clic en la siguiente URL para ver:
http://helpdesk/CAisd/pdmweb.exe?OP=SEARCH+FACTORY=chg+SKIPLIST=1+QBE.EQ.id=40072
3
```

Para agregar un comentario al incidente, conteste este correo o incluya la línea siguiente (en una sola línea).

%incident_id=1234

Este correo electrónico y los archivos que se transmiten con él son para el uso exclusivo de los destinatarios deseados y contienen información que puede ser privilegiada y confidencial. Quedan prohibidas la revisión, utilización, divulgación o distribución no autorizadas. Si usted no es el destinatario deseado de este correo electrónico, suprimalo junto con los archivos transmitidos y notifíquelo al remitente inmediatamente.

Lista de destinatarios de notificación manual

Puede configurar un conjunto predeterminado de destinatarios disponibles que la página de composición de notificación manual presenta para solicitudes, incidentes y problemas. Los destinatarios disponibles hacen más eficiente el proceso de notificación manual para los analistas porque se puede configurar una lista de objetos de contacto (por ejemplo, el usuario final afectado) o nombres del contacto individual para facilitar el uso como destinatarios de notificaciones manuales.

Al agregar un destinatario de contacto de objeto se agregan los nombres del contacto individual que el contacto de objeto representa en la lista de destinatarios (consolidando cualquier entrada duplicada). Se puede hacer referencia al mismo contacto varias veces para diferentes objetos de contacto como Asignatario y Usuario final afectado. Algunas entradas, como el objeto de contacto de Lista de responsables, pueden agregar varias entradas a la lista de destinatarios.

Los contactos y los objetos de contacto se quedarán en la lista de destinatarios disponibles después de que los agregue a la lista. Este comportamiento permite eliminar destinatarios sin afectar a la lista original de destinatarios disponibles.

Ejemplo: cómo funciona la lista de destinatarios disponibles

Los siguientes ejemplos demuestran cómo perfeccionan los destinatarios predeterminados el proceso de notificación de actividad manual.

Los destinatarios de contacto de objeto incluyen las siguientes entradas:

- El usuario A pertenece a los objetos de contacto "asignatario" y "usuario final afectado".
- La lista de responsables incluye varios nombres de contacto. Por ejemplo, usuario B y usuario C.

Puede realizar las siguientes acciones:

- Agregar objetos de contacto que se refieren tanto al usuario A como a la lista de destinatarios.
Solamente aparece una entrada de usuario A en la lista de destinatarios.
- Eliminar accidentalmente al usuario A de la lista de destinatarios.
No tiene que hacer referencia al ticket para obtener el nombre del usuario A y buscarlo para volverlo a agregar. Puede agregar rápidamente al usuario A a la lista de destinatarios porque éste figura en la lista de destinatarios disponibles.
- Eliminar accidentalmente un nombre de contacto, como el usuario C, de la lista de destinatarios que procede de la lista de responsables.
Puede agregar la lista de responsables desde los destinatarios de contacto de objeto para volver a agregar el nombre de contacto. Dado que las entradas duplicadas se consolidan, los demás contactos en la lista de responsables que no se suprimieron de la lista de destinatarios no se verán afectados.

Notificaciones de asignatario anteriores

Puede definir los valores de Asignatario o Grupo anteriores para una notificación de actividad que detecta cambios en campos clave cuando se guarda un ticket. Los valores anteriores le permiten notificar a un asignatario anterior cuándo un ticket se transfiere, o notificar a los grupos actuales y anteriores cuándo se escala la prioridad de un ticket.

Los campos de valor anterior de un ticket son campos locales que existen solamente en la memoria y no en la base de datos. Los campos se rellenan durante el almacenamiento de un ticket y se borran en la terminación del procesamiento de notificación. Un campo de valor anterior se asocia con un tipo de actividad particular a través de una asociación de actividades.

Puede definir valores anteriores que detectan cambios a los siguientes campos clave de un ticket:

Campo	Solicitudes, incidentes, problemas	Solicitudes de cambio	Incidencias
Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución	Sí	Sí	Sí

Campo	Solicitudes, incidentes, problemas	Solicitudes de cambio	Incidencias
y el número de ejecuciones.			
Activo	Sí	Sí	Sí
Asignado	Sí	Sí	Sí
Área/Categoría de solicitud	Sí	Sí	Sí
Group	Sí	Sí	Sí
Impacto	Sí	Sí	Sí
Prioridad	Sí	Sí	Sí
Urgencia	Sí	No	No
Severidad	Sí	No	No

Hay varios contactos que puede especificar para cada tipo de objeto (solicitud, incidente, problema, orden de cambio o incidencia), que notifican a los contactos actuales y anteriores cuando ocurre una actividad.

- **Asignatario:** persona asignada para manejar el ticket.
- **Asignatario anterior:** persona previamente asignada para manejar el ticket.
- **Grupo:** grupo asignado para manejar el ticket.
- **Grupo anterior:** grupo previamente asignado para manejar el ticket.

Después de que la regla de notificación se guarde, los campos Asignatario anterior y Grupo aparecen en la página Lista de notificaciones de contacto del objeto.

Ejemplo: configuración de valores actuales y anteriores para los campos clave

El siguiente ejemplo de uso describe cómo un administrador configura los valores actuales y anteriores para los campos clave a fin de garantizar que el representante de soporte anterior sea notificado cuando una solicitud se transfiere a otra persona.

1. **Situación:** los representantes de soporte se frustran porque un ticket se transfirió a otras personas y nunca fueron notificados.
2. **Tarea:** el administrador agrega los contactos del objeto Asignatario y Asignatario anterior a la regla de notificación para la notificación de actividad de transferencia. Adjuntan una plantilla de mensaje y especifican los asignatarios anteriores y actuales para notificar en el formulario de solicitud.

3. **Acción:** cuando la solicitud se guarda, se rellenan los campos Asignatario y Asignatario anterior de la solicitud. Cuando la actividad ocurre (se transfiere el ticket), se evalúa la condición para la regla.
4. **Resultado:** si se cumple la condición, un mensaje de notificación que describe la actividad del ticket se envía al asignatario actual y al asignatario anterior.

Ejemplo de notificación a los contactos sobre la transferencia de un ticket

Puede notificar a los contactos actuales y anteriores cuando se transfiere un ticket de CA Service Desk Manager.

Ejemplo: notificación a los contactos actuales y anteriores sobre la transferencia de un ticket

1. En la ficha Administración, vaya a Notificaciones, Notificaciones de actividades.
Aparecerá la página Lista de notificaciones de actividades.
2. Seleccione la notificación de actividad de transferencia.
Aparecerá la página Detalles de notificación de actividad de transferencia.
3. En el campo Tipo de objeto, seleccione Solicitudes/Incidentes/Problemas.
4. En la ficha Reglas de notificación, en Símbolo, seleccione la regla de notificación de transferencia predeterminada.
Aparecerá la página Regla de notificación de transferencia predeterminada.
5. En la ficha Contactos del objeto, haga clic en Actualizar contactos de objeto.
6. Haga clic en Buscar.
Aparecerá la página Destinatarios de actualización de reglas de notificación.
7. En la lista Contactos del objeto, seleccione Asignatario y Asignatario anterior en la lista de la izquierda y haga clic en el botón de selección de contactos ($\geq$).
El elemento seleccionado se agrega a la lista de la derecha.
Nota: Utilice las teclas CTRL o MAYÚS más el botón izquierdo del ratón para seleccionar varios contactos de objetos.
8. Haga clic en OK.
9. Guarde la regla de notificación.
La lista Contactos del objeto muestra el contacto de objeto seleccionado.
10. En la página Regla de notificación de transferencia predeterminada, haga clic en Plantilla de mensaje. Seleccione una plantilla y asegúrese de que la opción Notificación automática esté habilitada.

11. Cree una solicitud, especifique un Asignatario y haga clic en Guardar.
12. En la página Detalles de solicitud, seleccione Actividades y, a continuación, Transferir en el menú Archivo.
13. Especifique un nuevo Asignatario y haga clic en Guardar.
Se envía la notificación a los asignatarios actuales y anteriores cuando se lleva a cabo la transferencia.

Notificaciones de elementos de configuración

Un elemento de configuración le permite definir una notificación de actividades que se asocia con un elemento de configuración específico que, a su vez, se asocia con un ticket de CA Service Desk Manager específico. Esta función le permite seguir información sobre los usuarios, las organizaciones y los distribuidores de un elemento de configuración.

Puede especificar los contactos de objeto de CI en la página Receptores de actualización de reglas de notificación, como CI Org mant, CI Contacto primario y así sucesivamente.

Ejemplo de notificación al contacto primario de un elemento de configuración sobre una incidencia

Puede definir una notificación de actividades para un contacto primario que se envíe para un elemento de configuración específico para un ticket de CA Service Desk Manager específico.

Ejemplo: notificación al contacto primario de un elemento de configuración sobre una incidencia

1. En la ficha Administración, vaya a Notificaciones, Notificaciones de actividades.
Aparecerá la página Lista de notificaciones de actividades.
2. Seleccione la notificación de actividades inicial de la lista.
Aparecerá la página Detalles de notificaciones de actividades iniciales.
3. Seleccione el tipo de objeto que desea utilizar:
4. En la ficha Reglas de notificación, seleccione el vínculo de la regla de notificación predeterminada.
Aparecerá la página Regla de notificación predeterminada.
5. Seleccione el vínculo Plantilla de mensaje predeterminado, asegúrese de que la opción Notificación automática está habilitada.
6. Seleccione la ficha Contactos del objeto y haga clic en Actualizar contactos de objeto.

Aparecerá la página Búsqueda de notificaciones de contactos de objetos.

7. Haga clic en Buscar. Aparecerá una lista de contactos de objetos.
8. Seleccione los contactos primarios del elemento de configuración en la lista de la izquierda y haga clic en el botón de selección de contactos ($\geq$).

El elemento seleccionado se agrega a la lista de la derecha.

Puede utilizar las teclas CTRL o MAYÚS más el botón izquierdo del ratón para seleccionar varios contactos de objetos. Puede agregar un objeto para una solicitud y varios objetos para una orden cambios o incidencia.

El contacto de objeto está en la lista de la derecha.

9. Haga clic en OK.
10. Guarde la regla de notificación.

La lista Contactos del objeto muestra el contacto de objeto seleccionado.

11. Lleve a cabo las siguientes tareas:

- En la ficha Service Desk, cree o actualice un elemento de configuración existente.
- Agregue el contacto principal mostrado en la ficha Contactos del objeto. El contacto de objeto seleccionado aparecerá en la página Detalles del elemento de configuración.
- Agregue el elemento de configuración a la incidencia.

Cuando esta actividad se lleva a cabo, se implementa la regla y se evalúa la condición. Si se cumplen los criterios para la condición, un mensaje de notificación que describe la actividad de ticket se envía a todos los contactos del elemento de configuración asociados con esta regla de notificación.

Asignación de miembros al Grupo de CAB

La página Actualización de miembros le permite asignar miembros a un grupo de CAB.

Procedimiento para asignar miembros al grupo de CAB

1. En la página Detalles de grupo, seleccione la ficha Miembros.
2. Haga clic en Actualizar miembros.

Aparecerá la página Búsqueda de contactos.

3. Introduzca los criterios de búsqueda para mostrar los contactos deseados y haga clic en Buscar.

Aparecerá la página Actualización de miembros, que muestra los contactos que coinciden con los criterios de búsqueda.

4. Seleccione en la lista de la izquierda los contactos que desee asignar a este grupo. Para seleccionar varios elementos, mantenga pulsada la tecla Ctrl mientras hace clic con el botón izquierdo del ratón.

5. Cuando haya seleccionado todos los contactos que desee, haga clic en el botón de selección ($\geq$).

Los contactos seleccionados se mueven a la lista de miembros a la derecha.

6. Haga clic en OK.

Aparecerá la página Detalles de grupo, que muestra los contactos seleccionados en la ficha Miembros.

Notificaciones de encuestas

Para una notificación de actividad, puede definir detalles de notificación de encuesta separados para tickets, encuestas gestionadas, documentos de conocimiento y comentarios de conocimiento y enviárselos al cliente que iniciaba la actividad.

Mediante notificaciones de encuesta, puede hacer lo siguiente:

- Especifique una nueva encuesta o utilice una de las encuestas predeterminadas disponibles con el producto.
- Use los métodos de notificación que describen cómo se envían los mensajes de notificación a los usuarios.
- Defina un mensaje de encuesta para el cliente.

Cuando un cliente recibe la notificación de alguna encuesta, se incluye automáticamente una dirección URL en el cuerpo del mensaje en la que se puede hacer clic para acceder al formulario de la encuesta en el explorador Web y poder rellenarlo.

Se genera un registro de actividades tanto al enviar la notificación de estudio como al recibir el estudio del cliente.

Más información:

[Definición de notificaciones de encuesta](#) (en la página 195)

Cómo agregar hipervínculos de URL a las notificaciones

El campo `web_url` de las tablas `Change_Request` y `Workflow_Task` contiene un valor de dirección URL que permite al usuario acceder a una orden de cambios o una tarea del workflow en particular por medio de la interfaz Web. Si se emplea para las notificaciones por correo electrónico, basta con hacer clic en la dirección URL e ir a la interfaz Web sin que haga falta ejecutar ninguna otra consulta.

Para poder utilizar los hipervínculos de URL en las notificaciones, configure el sistema de la siguiente manera:

1. Instalar y configurar la interfaz Web de CA Service Desk Manager.

Note: Si desea obtener más información, consulte la *Guía de implementación*.

2. Con el Gestor de opciones, configure e instale la opción `web_cgi_url` a fin de especificar la ubicación del motor Web de CA Service Desk Manager, por ejemplo, `http://hostname/scripts/pdmcgi.exe`.

Más información:

[Uso del Gestor de opciones](#) (en la página 355)

Lector del registro de notificaciones

El lector del registro de notificaciones muestra las notificaciones que ha recibido el usuario que inició sesión por fecha, urgencia y estado. Con el Lector del registro de notificaciones, puede hacer lo siguiente:

- Cambie el orden de clasificación y establezca las opciones de menú de manera que el lector del registro de notificaciones aparezca automáticamente cada vez que se reciban mensajes nuevos.
- Haga doble clic doble en un mensaje de notificación para solicitar que CA Service Desk Manager muestre la página de detalles para el ticket asociada a la notificación.
- Controle los mensajes de notificación mediante la introducción de criterios de selección específicos. Al hacerlo, se ejecuta una consulta en la base de datos para realizar un análisis o para seleccionar los mensajes de notificación que coincidan con los datos especificados en los campos. Por ejemplo, se puede solicitar que se muestre una lista sólo de las notificaciones que no se hayan borrado cambiando el valor del campo Estado de mensaje a No borradas.
- Borre los mensajes de notificación para lograr mantener una lista de notificaciones con un tamaño manejable. Aunque las notificaciones borradas no se muestran al acceder inicialmente al lector de registro de notificaciones, se puede optar por verlas si es necesario.

Cómo establecer las opciones del lector del registro de notificaciones

El lector del registro de notificaciones dispone de varias opciones con las que se puede definir cómo se notifica la recepción de mensajes nuevos.

Procedimiento para establecer las opciones del lector del registro de notificaciones

1. En la ficha ServiceDesk, vaya a Ver, Lector de registro.
Aparece la página Lector de registro de notificaciones.
2. Utilice la casilla de verificación a la izquierda de cada notificación para establecer las opciones siguientes. Puede seleccionar elementos para realizar operaciones como Borrar selección o Suprimir selección.

Encabezado

Muestra el encabezamiento del mensaje, que normalmente contiene el número del ticket y el tipo de actividad.

Fecha de inicio

Muestra la fecha y la hora en las que se ha enviado la notificación a la ventana del lector del registro.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Muestra el estado de la notificación.

Urgencia

Define el nivel de urgencia de la notificación (bajo, normal, alto o emergencia), que indica la importancia relativa de distintas actividades. Los niveles de urgencia están predefinidos; sin embargo, el administrador del sistema es responsable de configurar otros aspectos de la notificación, como los métodos de notificación y las asociaciones de actividad. El administrador del sistema define también el método de notificación que se emplea para los contactos y grupos en cada nivel de urgencia.

Texto de mensaje

El texto completo del mensaje de notificación.

El lector del registro muestra cualquier cambio.

3. Haga clic en Cerrar.

La página Lector de registro de notificaciones cierra y las opciones se establecen.

Respuestas personalizadas

Puede crear respuestas personalizadas y adjuntarlas a registros de solicitudes, incidencias y órdenes de cambio al agregar actividades al registro. Por ejemplo, puede adjuntar respuestas personalizadas en las ventanas Cambio de estado o Registrar comentario a las que se accede desde el menú Actividades.

Creación de una respuesta personalizada

Puede crear una respuesta personalizada para añadir a solicitudes, incidencias y registros de orden de cambio.

Procedimiento para crear una respuesta personalizada

1. En la ficha Administración, desplácese hasta Service Desk, Respuestas personales.
Aparecerá la página Lista de respuestas personales.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nueva respuesta personalizada.
3. Rellene los campos de la página.

Propietario de la respuesta

Especifica el contacto que posee la respuesta. Si este campo se deja vacío, la respuesta está disponible para todos los analistas.

Respuesta

Especifica el texto enviado a todos los que reciben esta respuesta. Este campo puede tener una extensión máxima de 1000 caracteres.

Puede utilizar variables en este campo, por ejemplo:

ref_num del ticket: @{call_req_id.ref_num}
Asignatario: @{call_req_id.assignee.combo_name}
Cliente: @{call_req_id.customer.combo_name}
Descripción: @{call_req_id.description}

4. Seleccione el tipo de registro para el que desea que esta respuesta esté disponible. Haga clic en Guardar.

Se crea una respuesta personalizada.

Sustitución de variables de respuestas individualizadas

Las variables pueden estar incrustadas en el texto de una respuesta personal. Estas variables permiten que se sustituya información de la solicitud, orden de cambios, incidencia, problema o incidente correspondiente. La sintaxis de las variables es la misma que la utilizada en todo el producto CA Service Desk Manager, como en las plantillas de mensajes de notificación de actividades y el texto de mensaje de actividad de notificación manual. Esta información sólo puede ser sustituida de la solicitud, orden de cambios, incidencia, problema o incidente correspondiente. Las plantillas de mensajes de notificación de actividades y el texto de mensaje de actividad de notificación manual permiten que también se incluya información del registro de actividades.

Las casillas de verificación para cada tipo de objeto (solicitudes, órdenes de cambios, incidencias, incidentes y problemas) permiten que se filtren las respuestas durante la selección. Si el tipo de objeto no está activado, la respuesta no estará disponible para ese objeto. Por ejemplo, si sólo se activa la casilla de verificación Solicitud, la respuesta únicamente aparecerá en las actividades de una solicitud.

Una sola respuesta puede utilizarse con todos los tipos de objeto (solicitudes, órdenes de cambios, incidencias, problemas e incidentes). Dado que cada objeto tiene atributos diferentes, no se sustituye la información que no se aplica al objeto (por ejemplo, intentando sustituir el número de solicitud en una respuesta a una incidencia).

Un ejemplo de texto de respuesta y las sustituciones variables que ocurren para cada tipo de objeto es:

```
Ésta es la solicitud nº '@{call_req_id.ref_num}'  
Ésta es la orden de cambios nº '@{change_id.chg_ref_num}'  
Ésta es la incidencia nº '@{issue_id.ref_num}'
```

En el caso de *solicitudes*, se produce la siguiente sustitución:

```
Ésta es la solicitud nº 'cr_demo:11'  
Ésta es la orden de cambios nº ''  
Ésta es la incidencia nº ''
```

En el caso de *órdenes de cambios* se produce la siguiente sustitución:

```
Ésta es la solicitud nº ''  
Ésta es la orden de cambios nº 'chg_demo:3'  
Ésta es la incidencia nº ''
```

En el caso de *incidencias*, se produce la siguiente sustitución:

```
Ésta es la solicitud nº ''  
Ésta es la orden de cambios nº ''  
Ésta es la incidencia nº 'iss_demo:6'
```

Si se utilizan las casillas de verificación Mostrar esta respuesta para, pueden crearse distintas versiones de una respuesta con las variables de sustitución adecuadas para el objeto correspondiente (solicitudes, órdenes de cambios, incidencias, problemas o incidentes).

El formato de las variables de sustitución de los distintos objetos es el siguiente.

Objeto	Formato de variable
Solicitud/incidente/problema	@{call_req_id.attr}
Orden de cambios	@{change_id.attr}
Incidencia	@{issue_id.attr}

La sustitución se produce cuando se copia la respuesta en el campo Descripción del usuario. La respuesta se copia después de seleccionarla de la lista desplegable Respuesta personalizada y que ésta se cierre.

Administración de correo electrónico

El correo electrónico le permite comunicarse con los usuarios finales, como empleados o clientes. Los usuarios finales pueden responder a notificaciones por correo electrónico para actualizar o crear tickets que utilizan el correo electrónico de un equipo u otro dispositivo como un teléfono móvil o smartphone. Por ejemplo, una respuesta a una notificación por correo electrónico enviada a un usuario final para obtener información adicional puede actualizar un ticket con la información pedida.

Las siguientes funciones controlan la comunicación de correo electrónico desde y para el usuario final:

- **Notificaciones por correo electrónico:** controla el correo electrónico saliente.

Tenga en cuenta la siguiente información sobre el correo electrónico saliente:

- El daemon de correo (pdm_mail_nxd) envía notificaciones de correo saliente, utilizando el protocolo de transferencia simple de correo (SMTP).
- Configure las opciones de SMTP del servidor de correo mediante Gestor de opciones, Correo electrónico.
- Puede utilizar métodos de notificación por correo electrónico predeterminados (o configurar nuevos métodos) para enviar correo directamente al receptor por correo SMTP.

- **Buzones de correo:** controla el correo electrónico entrante.

Tenga en cuenta la siguiente información sobre el correo electrónico entrante:

- El receptor de correo (pdm_maileater_nxd) recupera correo electrónico entrante para crear y actualizar tickets usando el protocolo de oficina de correo (POP3) o el protocolo de acceso a correo de Internet (IMAP o IMAP4).
- Los buzones de correo de CA Service Desk Manager definen las cuentas de correo electrónico (bandejas de entrada).
- Las reglas para el buzón de correo definen cómo cada buzón de correo controla el correo entrante.

Más información:

[Notificaciones por correo electrónico](#) (en la página 101)

Buzones de correo

CA Service Desk Manager proporciona un buzón de correo predeterminado que se conecta al servidor de correo y que requiere configuración adicional como valores de configuración para el nombre de host, nombre de usuario, contraseña, etc.

Algunas de las formas en las que puede definir un buzón de correo para tratar correo entrante son las siguientes:

- Configure un buzón de correo para utilizar el protocolo IMAP o POP3.
- Cree múltiples buzones de correo para permitir que organizaciones o clientes individuales tengan buzones de correo diferentes, con comportamientos separados para cada uno.
- Use las reglas para el buzón de correo para filtrar mensajes y establecer comportamiento específico, definir respuestas automáticas y establecer acciones específicas (por ejemplo, actualizar tickets), basado en el contenido y las propiedades del mensaje.
- Use las reglas para el buzón de correo para proporcionar valores predeterminados del API de texto y establecer interfaces de correo electrónico con otro software. Puede configurar parámetros (como categoría, asignatario, etc.) específicamente para la interfaz.
- Utilice frases de notificación en las reglas para el buzón de correo a fin de crear elementos comunes para respuestas automáticas a través de múltiples reglas.
- Use las políticas de buzón de correo para ayudar a proteger contra abuso basado en correo.

Más información:

[Sondeo de buzón de correo](#) (en la página 103)

Reglas de buzón de correo

Las reglas para el buzón de correo permiten configurar algunas acciones, respuestas, o ambas, que deben producirse para mensajes recuperados de un buzón de correo. La tabla (usp_mailbox_rule) mantiene las reglas que se aplican a la conexión para cada cuenta del servidor de correo (usp_mailbox). Las reglas pertenecen a buzones de correo específicos. Puede suprimir las reglas o hacerlas inactivas para deshabilitarlas.

Nota: Cuando se crean reglas para el buzón de correo, es posible asociarlas con un buzón de correo específico (otro buzón de correo no puede compartir esas reglas). Si desea utilizar reglas que pertenezcan a un buzón de correo para otro buzón de correo, vuelva a crearlas para el otro buzón.

Las reglas para el buzón de correo también permiten realizar lo siguiente:

- Especificar diversos comportamientos para los mensajes de cada buzón de correo, basado en la base del contenido de los mensajes.
- Proporcionar parámetros predeterminados del API de texto (como categoría, asignatario, etc.) para procesar y enrutar mensajes.
- Establecer filtros de mensaje basado en expresiones regulares y palabras clave fijas.
- Utilizar una frase de notificación común para las respuestas automáticas a numerosas definiciones de regla para el buzón de correo, como en el ejemplo siguiente:

Gracias por enviar su solicitud.
@{notification_phrase[RequestReply].phrase}

La frase aparece en las respuestas a correo electrónico enviadas a todos los buzones de correo incluidos en la regla.

Más información:

[Acciones de regla de buzón de correo](#) (en la página 136)

[Coincidencia de patrones en reglas de buzón de correo](#) (en la página 136)

[Filtrado de restricciones de identificador del objeto de cadena](#) (en la página 138)

[Caracteres especiales en expresiones regulares](#) (en la página 140)

[Texto de muestra para frases de notificación en una regla de buzón de correo](#) (en la página 141)

Acciones de regla de buzón de correo

Las reglas de buzón de correo permiten realizar cualquiera de las siguientes acciones de correo electrónico:

- Ignorar correo electrónico: no se procesa el correo electrónico y no se responde.

Esta acción es útil para mensajes de nivel de sistema como Fuera de la oficina o los errores de entrega de correo.

- Ignorar correo electrónico y responder: no se procesa el correo electrónico ni las respuestas al remitente. Los correos electrónicos de respuesta utilizan los mensajes de respuesta satisfactorios y se ignoran los mensajes de respuesta con errores.

- Actualizar objeto: se utiliza la cadena de filtro para determinar el identificador de objeto (por ejemplo, %Incident:{{object_id}}% en el correo electrónico) y se envía una solicitud de actualización en Text API. Si no se encuentra el identificador de objeto, Text API no hace nada.

Esta acción normalmente trata las respuestas de correo electrónico en las que el identificador de objeto se incrusta en el correo electrónico. Si ningún identificador de objeto está presente, el mensaje de respuesta de fallo suele enviarse.

- Crear/actualizar objeto: se utiliza la cadena de filtro para determinar el identificador de objeto (por ejemplo, %Incident:{{object_id}}% en el correo electrónico) y se envía una solicitud de actualización en Text API. Si se encuentra el identificador de objeto, Text API actualiza un ticket. Si no se encuentra el identificador de objeto, Text API crea un ticket.

Esta acción es el comportamiento estándar del daemon de correo (Mail Eater) en el cual el correo electrónico contiene o no palabras clave de Text API.

Nota: Para obtener información sobre cómo configurar reglas para el buzón de correo, consulte la *Ayuda en línea*.

Coincidencia de patrones en reglas de buzón de correo

Las reglas para el buzón de correo utilizan expresiones regulares para la coincidencia de patrones. Considere los siguientes caracteres de espacio en blanco que se aplican a expresiones regulares en reglas para el buzón de correo:

\t

Especifica una ficha horizontal.

\r

Especifica un carácter de retorno de carro.

\n

Especifica un carácter de línea nueva o salto de línea.

Los caracteres que representan saltos de línea en un texto pueden variar con el sistema operativo, servidor de correo y cliente de correo, por ejemplo:

- UNIX utiliza \n.
- Microsoft utiliza \r\n
- Macintosh utiliza \r
- MacOS X utiliza \n.

En ciertas circunstancias, los elementos de procesamiento de correo de CA Service Desk Manager intercambian o sustituyen uno de estos caracteres de salto de línea por otro para establecer o mantener una distinción entre diferentes elementos de texto, como texto de mensaje y parámetros adjuntos. En consecuencia, cuando desee utilizar un salto de línea o párrafo, cree los filtros para que \r y \n puedan coincidir, sea cual sea el que se encuentre. Si desea indicar un salto de línea entre dos palabras clave, cree los filtros para que una secuencia de uno o más caracteres \r y \n pueda coincidir.

El ajuste de líneas por parte del cliente de correo que envía un mensaje puede hacer que aparezcan saltos de línea inesperados en medio del texto que debería coincidir con la cadena de filtro, cuando la cadena de filtro busca el cuerpo del mensaje. Un espacio puede cambiar a un retorno de carro, salto de línea, o ambos, o bien el retorno de carro, salto de línea, o ambos, pueden insertarse después de un espacio. Si un mensaje se compone en HTML y contiene listas numeradas o con viñetas, o párrafos con sangría, las tabulaciones también pueden aparecer después de que el cliente de correo convierta y envíe el mensaje. Cuando incluya espacios en medio de una cadena de filtro, utilice un bloque de expresión regular que represente cualquier espacio en blanco de tamaño variable. Este bloque es [\t\r\n]+ (paréntesis de apertura, espacio, barra diagonal inversa, t, barra diagonal inversa, r, barra diagonal inversa, n, paréntesis de cierre, signo de más) y representa cualquier secuencia de uno o más espacios, tabulaciones, retornos de carro y saltos de línea.

Ejemplo: uso de [\t\r\n] para coincidir con una palabra clave de forma exacta

Este ejemplo demuestra cómo puede utilizar caracteres de espacio en blanco para que coincidan con la palabra clave "condición" y no con otras posibles palabras clave como las siguientes:

condicional
condicionamiento
incondicional
acondicionar

Para coincidir solamente con la palabra clave condición, empiece y siga la palabra clave con uno o más caracteres de espacio en blanco de la siguiente forma:

```
[\\t\\r\\n]condición[ \\t\\r\\n]
```

Mail Eater coincide solamente con la palabra condición o la palabra como parte de una frase, y no como parte de otra palabra como incondicional.

Filtrado de restricciones de identificador del objeto de cadena

Las restricciones se aplican a las cadenas de filtrado de reglas para el buzón de correo que determinan el identificador de objeto (por ejemplo, %Incident:{{object_id}}%) en un correo electrónico. El texto que rodea un identificador de objeto ({{object_id}}) debe ser inequívoco tanto en contenido como en longitud; el texto debe definir claramente el inicio y final del valor de artefacto de ID del ticket que está entre el texto.

Las restricciones siguientes se aplican a cómo el receptor de correo interpreta el *inicio* del valor del artefacto de ID del ticket:

- El marcador de posición {{object_id}} no debe ser el primer elemento en la cadena de filtrado. Se requiere por lo menos un carácter y generalmente una palabra clave distintiva, o una secuencia de letras, números y símbolos debe preceder la palabra clave del ID del objeto.
- El carácter que inmediatamente precede al marcador de posición {{object_id}} no debe ser un carácter repetible u opcional (lo que significa, un carácter seguido por un signo más (+), un asterisco (*) o un signo de interrogación (?)) que puede ser parte de un valor de artefacto del ID del ticket. Los caracteres repetibles u opcionales pueden confundirse con el principio del valor de artefacto del ID del ticket, a menos que sean caracteres de espacios en blanco. Los caracteres de espacios en blanco (espacio, tabulación, retorno de carro, salto de línea) no deben ser parte de un valor de artefacto de ID de ticket.
- El carácter que inmediatamente precede al marcador de posición {{object_id}} no debe ser un conjunto de caracteres entre paréntesis repetible u opcional que incluye caracteres que pueden ser parte de un valor de artefacto del ID del ticket.

Las siguientes restricciones se aplican a cómo el receptor de correo interpreta la *longitud* del valor del artefacto del ID del ticket:

- El marcador de posición `{{object_id}}` no debe ser el último elemento de la cadena de filtrado. Uno o más caracteres deben seguir al marcador de posición `{{object_id}}`.
- El carácter que inmediatamente sigue al marcador de posición `{{object_id}}` no debe ser un carácter repetible u opcional (lo que significa, un carácter seguido por un signo más (+), un asterisco (*) o un signo de interrogación (?)) que puede ser parte de un valor del artefacto del ID del ticket. Los caracteres repetibles u opcionales pueden confundirse con el final del valor del artefacto del ID del ticket, a menos que sean caracteres de espacios en blanco. Los caracteres de espacios en blanco (espacio, tabulación, retorno de carro, salto de línea) no deben ser parte de un valor de artefacto de ID de ticket.
- El primer carácter después del marcador de posición `{{object_id}}` no debe ser un carácter que pueda ser parte de un valor del artefacto del ID del ticket.
- Evite los caracteres siguientes inmediatamente antes y después del marcador de posición `{{object_id}}`:
 - Todas las letras minúsculas y mayúsculas
 - Los números
 - El signo más (+)
 - La barra diagonal (/)
 - La coma (,)
 - El punto (.), porque puede representar cualquier carácter excepto un salto de línea, y de esta forma, puede ser cualquiera de los caracteres de esta lista.

porque cualquiera de estos caracteres puede existir dentro del valor del artefacto del ID del ticket. Cuando un conjunto entre paréntesis (varios caracteres entre paréntesis, con cualquiera de los cuales la comprobación de filtro puede coincidir) precede o sigue al marcador de posición `{{object_id}}`, el conjunto entre paréntesis no debe contener ninguno de estos caracteres.

Caracteres especiales en expresiones regulares

La coincidencia de patrones para los filtros en reglas de buzón de correo sigue las reglas para expresiones regulares de ASCII con caracteres especiales de tipo C.

Importante: es recomendable que esté familiarizado con la sintaxis de Regex para utilizar caracteres especiales en expresiones regulares.

Por ejemplo, considere los siguientes caracteres especiales para patrones Regex que se aplican a expresiones regulares en reglas para el buzón de correo:

\t

Especifica una ficha horizontal. En cadenas de filtro para reglas de buzón de correo, \t coincide con el inicio y el final del texto (y las fichas) y es específico para Mail Eater.

\r

Especifica un retorno de carro (vuelve al inicio de la línea actual).

Nota: No utilice \r para buscar asuntos de mensajes ni direcciones de remitentes.

\n

Especifica una línea nueva (combinación de salto de línea y retorno de carro).

Nota: No utilice \n para buscar asuntos de mensajes ni direcciones de remitentes.

\t, \r y \n son los caracteres especiales que se producen más a menudo en expresiones regulares de reglas para el buzón de correo.

Ejemplo: uso de \t, \r y \n

`[ \t]solicitud[ \t]`

Busca texto para la palabra solicitud. Los paréntesis coinciden con cualquier carácter del conjunto, incluido el espacio, de modo que [\t] coincide con un espacio o tabulador.

`[ \r \n]+grave[ \t \r \n]`

Busca texto para la palabra grave al principio de una línea, al principio del mensaje o en todo el contenido de una línea. Los paréntesis coinciden con cualquier carácter del conjunto y el signo más (+) coincide con uno o más de los anteriores, de modo que [\r \n]+ coincide con uno o más retornos de carro y líneas nuevas.

Texto de muestra para frases de notificación en una regla de buzón de correo

Este ejemplo ofrece texto de muestra que se puede utilizar para incluir frases de notificación en una regla para el buzón de correo. Puede definir versiones independientes de una frase de notificación para texto sin formato y para HTML cuando la frase contiene algunos saltos de línea u otro formato.

Utilice el siguiente texto en Texto satisfactorio, HTML satisfactorio o ambos campos, en la página Actualizar regla para buzón de correo, ficha Respuesta satisfactoria:

- Texto satisfactorio

```
Gracias por enviar su solicitud.  
@{notification_phrase[IncidentURL1]}.phrase}  
@{notification_phrase[RequestReply]}.phrase}
```

- HTML satisfactorio

```
Gracias por enviar su solicitud.</p>  
@{notification_phrase[IncidentURL1H]}.phrase}</p>  
@{notification_phrase[RequestReplyHTML]}.phrase}</p>
```

Nota: Para obtener información sobre cómo configurar frases de notificación, consulte la *Ayuda en línea*.

Más información:

[Sintaxis de la frase de notificación](#) (en la página 120)

[Frases y códigos de notificación](#) (en la página 118)

Políticas de buzón de correo

Las políticas de buzón de correo protegen su organización contra ciertos tipos de abuso de correo electrónico. Puede implementarlas de las siguientes formas:

- Puede definir listas de exclusión e inclusión de direcciones de correo electrónico:
 - Las listas de inclusión limitan la recepción de correo electrónico sólo a correo que se envía desde direcciones de correo electrónico particulares (por ejemplo, usuario@compañía.com) o dominios de correo electrónico (por ejemplo, compañía.com).
 - Las listas de exclusión ordenan dominios de correo electrónico o direcciones de correo electrónico no deseadas.

La lista de inclusión predeterminada para cada buzón de correo es un asterisco (*). Un asterisco por sí mismo como un nombre completo en esta lista especifica el dominio mundial y representa todos los dominios de correo electrónico no incluidos en la lista de exclusión. Esta representación previene la ambigüedad de si la lista de inclusión es la lista completa de dominios permitidos o las excepciones a dominios en la lista de exclusión de la siguiente manera:

- Una lista de inclusión que incluye el dominio mundial especifica que todas las otras entradas de la lista de inclusión son excepciones a la lista de exclusión, y solamente se bloquean los dominios o las direcciones de la lista de exclusión (a excepción de direcciones específicas de la lista de inclusión).
 - Una lista de inclusión que no contiene el dominio mundial especifica que se permite el envío solamente de las direcciones y los dominios listados en la lista de inclusión, y solamente si la dirección o el dominio del remitente (si la dirección específica no está en la lista de inclusión) no están en la lista de exclusión.
- Puede establecer el límite máximo de mensajes por hora por dirección para la detección de denegación de servicio (DoS).

Mensajes máximos limita el número de correos electrónicos por hora que cualquier dirección de correo electrónico puede enviar a ese buzón de correo. Si una dirección de correo electrónico sobrepasa el límite, la dirección de correo electrónico se agrega a la lista de exclusión. No se procesa ningún mensaje más de la dirección de correo electrónico de ese remitente para ese buzón de correo hasta que elimine la dirección de correo electrónico de la lista de exclusión.

Las políticas de buzón de correo para las listas de inclusión y exclusión, y el número máximo de correos electrónicos permitidos por hora conciernen solamente al único buzón de correo asociado. Una dirección que se agrega automáticamente a una lista de exclusión de buzón de correo con la intención de infringir la restricción de número máximo de correos electrónicos no se agrega automáticamente a la lista de exclusión para ningún otro buzón de correo, como tampoco se usa el recuento de correo electrónico para otros buzones de correo.

Las direcciones de correo electrónico que infringen la política se registran en STDLOG sobre la base de las definiciones de log_policy_violation (Ninguno, Registrar primero o Registrar todo).

Cómo implementar los buzones de correo

CA Service Desk Manager proporciona un buzón de correo predeterminado (llamado Predeterminado) que está activo y que puede utilizar en su organización. Puede modificar el buzón de correo predeterminado, crear buzones de correo adicionales, o ambas cosas.

Para implementar buzones de correo, realice los siguientes pasos preliminares:

- Configure la cuenta de servidor de correo que quiere utilizar.
- Cree contactos y especifique sus direcciones de correo electrónico si no quiere permitir a los usuarios anónimos que creen y actualicen los tickets (opción Permitir anónimo).

Para configurar el buzón de correo predeterminado, realice los siguientes pasos básicos opcionales:

1. Edite el buzón de correo predeterminado.
2. Actualice las políticas y las reglas para el buzón de correo como sea apropiado.

El buzón de correo está activo y empieza el sondeo. El primer sondeo se produce después de un segundo.

Configuración del servidor de correo

Las notificaciones para un evento (notificación manual y automática) se envían con una sola definición de servidor de correo.

Procedimiento para configurar el servidor de correo

1. En la ficha Administración, vaya a Gestor de opciones, Correo electrónico.
Aparecerá la lista de opciones.
2. Haga clic en la opción que desea instalar.
Aparecerá la página Detalles de opciones.
3. Haga clic en Editar, complete los campos según sea necesario y haga clic en Instalar.
El servidor de correo se configura para enviar notificaciones (correo saliente).
4. Repita el procedimiento hasta que todas las opciones relevantes de la Lista de opciones estén configuradas.

Nota: Puede utilizar el comando `pdm_mail -F` y los parámetros `-T`, que establecen las direcciones del remitente y de respuesta, respectivamente. Al utilizar estos parámetros en métodos de notificación personalizados, las respuestas a las notificaciones recibidas de correo se pueden dirigir al buzón de correo apropiado.

Más información:

[pdm_mail Utility: enviar información por correo electrónico](#) (en la página 99)

Opciones de correo electrónico

La interfaz de correo electrónico envía notificaciones por correo electrónico y permite a los usuarios crear tickets a partir de un correo electrónico. Las opciones de correo electrónico permiten configurar los protocolos de correo salientes.

mail_from_address

Especifica la notificación de correo De: dirección. La dirección está en el formato Displayname<usuario@empresa.com>.

mail_login_password

Especifica la contraseña de inicio del servidor SMTP.

mail_login_userid

Especifica el ID de usuario de inicio de sesión del servidor SMTP.

mail_max_threads

Especifica el número máximo de conexiones SMTP simultáneas que pueden intentar comunicarse con el servidor.

mail_reply_to_address

Define la dirección de respuesta utilizada para las notificaciones por correo electrónico. Esta opción es útil si los correos electrónicos se envían desde la cuenta de un usuario, pero desea que las respuestas se envíen a otra dirección de correo electrónico. El valor predeterminado es el mismo que la dirección del remitente.

mail_smtp_domain_name

Define el nombre de dominio requerido por algunos servidores SMTP que comprenden los protocolos ESMTP. Puede borrar el nombre de dominio si establece el valor en NINGUNO.

mail_smtp_hosts

Especifica una lista de nombres de host SMTP separados por espacio para notificaciones por correo electrónico.

mail_smtp_host_port

Especifica un puerto SMTP para sustituir el puerto SMTP predeterminado.

mail_smtp_security_level

Especifica el nivel de seguridad SMTP. Estos son los valores válidos: 0=sin seguridad, 1=autenticación básica, 2=NTLM, 3=MD5 y 4=LOGIN. Si establece esta opción en 1, establezca las opciones mail_login_password y mail_login_userid. La mayoría de los servidores SMTP no requieren autenticación.

Editar el buzón de correo predeterminado

CA Service Desk Manager proporciona un buzón de correo predeterminado activo que puede editar para adaptarse a las necesidades de entrega de correo de su organización.

Para editar el buzón de correo predeterminado

1. En la ficha Administración, vaya a Correo electrónico, Buzones de correo. Aparece la lista Buzón de correo, que lista los buzones de correo activos.
2. Haga clic en Predeterminado en la columna Nombre. Aparece la página Detalles de buzón de correo predeterminado.
3. Haga clic en Editar.
4. Complete o actualice los otros campos como sea apropiado:

Secuencia

Especifica el número de secuencia de la regla. Los mensajes se comparan con reglas en orden de número de secuencia desde el más bajo al más alto.

Buzón de correo

Especifica el buzón de correo al cual pertenece esta regla.

Activo

Establece la regla como activa o inactiva.

Filtro

Especifica en qué parte del correo electrónico debe buscarse el patrón de filtro, por ejemplo, el contenido del asunto.

Cadena de filtro

Especifica una cadena de expresión regular con la que coincidir, por ejemplo [\t\r\n]request[\t\r\n]. El marcador de posición {{object_id}} le permite especificar el valor de artefacto para que el API de texto utilice con el fin de asociar el mensaje con un ticket específico.

Omitir mayúsculas y minúsculas

Especifica si se deben tener en cuenta las mayúsculas y minúsculas al hacer coincidir patrones.

Acción

Especifica la acción que debe tomarse cuando los criterios de filtro coincidan, por ejemplo, crear/actualizar el objeto.

Nota: Para obtener información sobre las acciones de regla, consulte la *Guía de administración*.

Objeto de acción

Muestra el tipo de objeto de ticket al cual se aplican las acciones de mensaje, por ejemplo, petición.

Tipo mínimo de artefacto

Establece el tipo de mínimo de comprobación de artefacto que quiere para permitir:

- **NINGUNO:** no especifica ninguna validación de artefactos. Este valor equivale a no agregar la palabra clave al archivo de entrada. También acepta comandos de ID de ticket del API de texto.
- **PROTEGIDO:** valida un ticket con respecto al hash para obtener confirmación. Si la confirmación falla, el artefacto se considera nulo y el filtrado realizado por el correo electrónico falla cuando busca un artefacto (`{{object_id}}`).
- **SEGURO:** valida el número de ticket desde un bloque de datos encriptado. Si el valor no es un número de ticket encriptado válido, el artefacto se considera nulo y el filtrado realizado por el correo electrónico falla cuando busca un artefacto (`{{object_id}}`).

Nota: Se permiten los tipos que son más seguros que aquellos que están establecidos. Dicho de otra manera, si establece el tipo mínimo en PROTEGIDO, se permiten ambos PROTEGIDO y SEGURO, pero no NINGUNO. Además, si se selecciona PROTEGIDO o SEGURO, no se aceptan los comandos de ID de ticket del API de texto.

Respuesta

Especifica un método de notificación para enviar una respuesta automática, por ejemplo, correo electrónico. Si no establece esta opción, no se devuelve ninguna respuesta. La respuesta, que está separada de cualquier notificación, indica que si las acciones ejecutadas para el mensaje tuvieron éxito o fallaron.

Asunto de la respuesta

Especifica un línea de asunto para la respuesta, por ejemplo, respuesta del Centro de servicio al usuario.

Escritura en stdlog

Escriba texto de correo electrónico en el registro estándar (stdlog) si el filtro coincide.

Prefijo de la entrada de registro

Especifica un prefijo para agregar al escribir texto de correo electrónico en las entradas del registro estándar. Utilice esta opción para habilitar entradas de registro coincidentes para las reglas.

Agregar línea de asunto

Agrega la línea de asunto del mensaje original al cuerpo del mensaje antes del procesamiento. Puede añadir, anteceder o no agregar una línea de asunto. Según cuáles sean las acciones para el mensaje, la línea de asunto se adjunta a la descripción del ticket o a un comentario del registro.

Valores predeterminados del API de texto

Especifica comandos predeterminados adicionales para el API del texto cuando el filtro coincide. Se combina con los contenidos de la sección [EMAIL_DEFAULTS] del archivo text_api.cfg.

Omisión de entradas del API de texto

Especifica detalles de ignorar adicionales para el API del texto cuando el filtro coincide. Se combina con los contenidos de la sección [EMAIL_IGNORE_INCOMING] del archivo text_api.cfg.

Detalles

Especifica información sobre la regla.

Texto satisfactorio

Especifica el contenido de texto sin formato de un mensaje de respuesta cuando el mensaje se procesa con éxito. Por ejemplo:

Gracias por enviar una actualización a su petición. Un técnico de soporte se pondrá en contacto con usted en las próximas 24 horas.

HTML satisfactorio

Especifica el contenido HTML de un mensaje de respuesta cuando el mensaje se procesa con éxito. Las siguientes opciones permiten editar texto HTML, así como obtener una vista previa de éste:

- **Editar HTML satisfactorio:** abre el editor HTML que puede utilizar para aplicar formato al HTML.
- **Vista rápida:** obtiene una vista previa del HTML.
- **Código fuente HTML:** muestra el código fuente HTML.

Texto erróneo

Especifica el contenido de texto sin formato de un mensaje de respuesta cuando el mensaje no se procesa con éxito.

HTML erróneo

Especifica el contenido HTML de un mensaje de respuesta cuando el mensaje no se procesa con éxito. Las siguientes opciones permiten editar texto HTML, así como obtener una vista previa de éste:

- **Editar HTML erróneo:** abre el editor HTML que puede utilizar para aplicar formato al HTML.
- **Vista rápida:** obtiene una vista previa del HTML.

Código fuente HTML: muestra el código fuente HTML.

5. (Opcional) Cree o actualice las políticas y las reglas de buzón de correo como sea apropiado.

Nota: Cuando se crean reglas para el buzón de correo, es posible asociarlas con un buzón de correo específico (otro buzón de correo no puede compartir esas reglas). Si desea utilizar reglas que pertenezcan a un buzón de correo para otro buzón de correo, vuelva a crearlas para el otro buzón.

Importante: recomendamos que establezca el buzón de correo asociado en inactivo antes de configurar una regla de buzón de correo. De lo contrario, los mensajes que recupere el servidor de correo entre el primer y el último cambio se procesarán con las reglas que estén vigentes al recuperar el mensaje.

6. Haga clic en Guardar.

Se guardan y aplican los cambios al buzón de correo predeterminado. El primer sondeo se produce después de un segundo.

Varios buzones de correo

CA Service Desk Manager puede procesar y gestionar múltiples buzones de correo. Cada buzón de correo puede tener su propia definición, en lugar de utilizar un único conjunto global de definiciones. Puede definir múltiples buzones de correo y utilizar diferentes plantillas o valores predeterminados para cada buzón de correo. Las definiciones múltiples permiten el uso por parte de clientes individuales de buzones de correo separados o les permite a ellos o a organizaciones utilizar buzones de correo diferentes y tener comportamientos diferentes para cada buzón de correo. Puede configurar múltiples buzones de correo utilizando la interfaz de administración. Cada buzón de correo utiliza las tablas siguientes:

- `usp_mailbox`: define el buzón de correo.

- **usp_mailbox_rule**: especifica un conjunto de reglas para cada buzón de correo.

Porque las reglas para el buzón de correo proporcionan valores predeterminados del API de texto, puede establecer interfaces de correo electrónico con otro software y otros parámetros (como categoría, asignatario, etc.) que se configuran específicamente para la interfaz.

Nota: Los servidores de IMAP admiten múltiples buzones de correo para una única cuenta, pero no se admiten buzones de correo alternativos; solamente se admite la bandeja de entrada predeterminada.

Cómo usan reglas varios buzones de correo

El componente receptor de correo (**pdm_maileater_nxd**) del servidor primario usa las reglas y las conexiones de buzón de correo para leer y procesar mensajes de una o más cuentas en uno o más servidores de correo. El receptor de correo procesa los buzones de correo en serie (solamente se procesa un buzón de correo por vez), y procesa las reglas en orden de número de secuencia.

Los buzones de correo múltiples utilizan las reglas de la siguiente manera:

1. Luego de la puesta en marcha del servidor primario, el receptor de correo lee las siguientes tablas:

usp_mailbox

Representa una conexión a un servidor de correo.

usp_mailbox_rules

Representa las reglas que se aplican a la conexión (**usp_mailbox**).

Contact_Method

Representa los métodos de contacto utilizados para contestaciones automáticas.

Document_Repository

Representa los repositorios de documentos para almacenar adjuntos.

El receptor de correo automáticamente detecta cambios a los objetos en cualquiera de estas tablas, incluso si se agregan objetos adicionales. Si se realiza un cambio a **usp_mailbox** o **usp_mailbox_rule**, el intervalo de sondeo para el buzón de correo afectado se reprograma a un segundo después de que se aplica el cambio.

2. En el intervalo definido por cada buzón de correo, el receptor de correo recupera cada correo electrónico de la bandeja de entrada para la cuenta asociada, y procesa el correo electrónico de la siguiente manera:
 - a. Comprueba la dirección de correo electrónico para detectar incumplimientos de política. Cuando el receptor de correo encuentra un incumplimiento, el procesamiento se detiene, y el registro estándar se ve afectado según la definición de buzón de correo.
 - b. Compara el correo electrónico con cada regla (mailbox_rule) que pertenece a ese buzón de correo.
 - c. Si se encuentra una regla coincidente, envía el mensaje al API de texto para que se publique, y responde al usuario como sea apropiado basado en la acción especificada para la regla.

Para responder a correos electrónicos, la cadena de filtro identifica el objeto y utiliza el API de texto para realizar el procesamiento. Después de que finaliza el procesamiento, la respuesta va a Respuesta o a Desde dirección.
 - d. Después de que el receptor de correo encuentra una regla que coincide, no se comprueba ninguna otra, y procesa el correo electrónico siguiente en la bandeja de entrada.
 - e. Si no se encuentra ninguna regla que coincida, el mensaje se descarta.
3. Después de que el receptor de correo procesa todos los correos electrónicos para una bandeja de entrada, los mensajes procesados y descartados se borran definitivamente del servidor de correo y se programa el siguiente intervalo de procesamiento.

Cómo configurar respuestas de correo electrónico

Las notificaciones por correo electrónico que utiliza en buzones de correo son específicas de las respuestas que se envían a un contacto en contestación de sus correos electrónicos. Puede configurar el correo electrónico para que cuando un contacto haga clic en un vínculo de respuesta en una notificación por correo electrónico, el correo electrónico de respuesta se remita a un buzón de correo.

Nota: Esta configuración difiere de las notificaciones por correo electrónico tradicionales.

Utilice Administración de CA Service Desk Manager para configurar el correo electrónico de la siguiente manera:

1. Cree un buzón de correo para tratar al correo electrónico entrante en un servidor.
2. Desplácese al Gestor de opciones, Correo electrónico, y configure el servidor de correo saliente.
3. (Opcional) Especifique una dirección de correo electrónico de notificación en la definición del contacto.
4. Desplácese a Notificaciones, Métodos de notificación, Correo electrónico, y cree o actualice un método de notificación que incluya las definiciones siguientes:

- Es compatible con SMTP: habilitado
- `pdm_mail [-F from_email_address] [-T reply_to_email_address]`

from_email_address

Especifica la dirección que se utiliza como la dirección emisora del mensaje. Esta dirección anula la dirección del remitente en la configuración del servidor de correo saliente.

reply_to_email_address

Especifica la dirección a la cual se envían las respuestas. Esta dirección anula la dirección a la que se responde en la configuración del servidor de correo saliente.

Cuando se establece una dirección de respuesta en la configuración del servidor de correo saliente y no se especifica ninguna dirección de respuesta en el método de notificación, se utiliza la dirección de respuesta en la configuración del servidor de correo saliente con ese método de notificación.

- Palabra clave "\$(REPLY_FROM)"

Si la palabra clave "\$(REPLY_FROM)" se especifica como cualquiera de las dos direcciones, esa dirección se elabora a partir del nombre de usuario y el nombre de host del servidor de correo electrónico para el buzón de correo. Esta palabra clave es válida solamente cuando una regla para el buzón de correo utiliza el método de notificación. Los métodos de notificación que la utilizan no se deben utilizar para ningún otro propósito. Por ejemplo, user name=dev, server name=mail32.ca.com, \$(REPLY_FROM)=dev@mail32.ca.com. Solamente utilice esta palabra clave si su servidor de correo está configurado para aceptar el nombre del servidor de correo como equivalente al nombre de dominio de correo electrónico. Utilice esta palabra clave con cautela: si el nombre de host no está extendido completamente en el dominio en la configuración del buzón de correo (por ejemplo, mailserver1 en lugar de mailserver1.customer7.com), el intérprete de campo no lo extiende automáticamente.

Nota: from_email_address y reply_to_email_address son las direcciones que aparecen en los encabezamientos De y Responder a del mensaje cuando el usuario lo lee. Si las direcciones son idénticas, puede especificar solamente la dirección from_address.

5. Desplácese a Correo electrónico, Reglas para el buzón de correo, abra cada regla para el buzón de correo aplicable y seleccione el nuevo método de respuesta en la lista desplegable Respuesta. Guarde cada regla actualizada.

Cuando el contacto responde a la notificación por correo electrónico, la respuesta se remite de manera predeterminada al buzón de correo especificado.

Más información:

[pdm_mail Utility: enviar información por correo electrónico](#) (en la página 99)

Identificación de dirección de remitente alternativa

Puede utilizar un parámetro -m en el asunto del mensaje para que CA Service Desk Manager identifique el remitente del mensaje mediante una dirección de correo electrónico diferente de la de aquél que originalmente lo envió. La palabra clave -m, seguida por un espacio y por la dirección de correo electrónico que CA Service Desk Manager reconoce, debe consistir en los últimos elementos de la línea de asunto. Considere la información siguiente cuando utilice el parámetro -m en el asunto:

- Tanto la dirección emisora real como la dirección alternativa que se especifica con -m se verifican en las listas de inclusión y exclusión.
- La dirección de correo electrónico que se especifica como la dirección alternativa debe contener solamente la dirección, y no el nombre para mostrar que la acompaña.
- Si más de una palabra sigue al parámetro -m en la línea de asunto, la dirección alternativa no se reconoce.

Artefactos

Un *artefacto* de correo electrónico remite a algo que surge del proceso de correo, por ejemplo, una dirección de correo electrónico que se incluye en un correo electrónico reenviado. El API de texto usa artefactos que contienen un ID de ticket (como un número de referencia) para admitir respuestas. Cuando se encuentra el ID del ticket, una palabra clave del API de texto existente (como %INCIDENT_ID) se establece y agrega a la entrada para el API de texto. El receptor de correo identifica que una respuesta se asocia con un ticket particular encontrando el artefacto en el mensaje.

Las reglas para el buzón de correo le permiten especificar el artefacto y el valor que el API de texto utiliza. Por ejemplo, puede definir una regla para incidentes como Incident:{{object_id}}%. Cuando una regla encuentra Incident:1234, el API de texto utiliza %INCIDENT_ID=1234 (1234 es el ref_num para el incidente). Porque el artefacto debe ser único en un correo electrónico y fácil de encontrar, puede hacer que el artefacto se diferencie más, como por ejemplo, %Incident:{{object_id}}%. A {{object_id}} deben seguirle un signo de porcentaje (%), un espacio o algún otro carácter que no pueda aparecer en un valor del artefacto. Las letras minúsculas y mayúsculas, los números, las barras diagonales, las comas y el signo más pueden ser parte de un valor. Los artefactos seguros se codifican mediante Base64 después de la encriptación. Si no utiliza artefactos seguros, los caracteres que siguen al artefacto no deben formar parte del sufijo del ID de ticket, si lo hubiere, que ha sido configurado para ese tipo de ticket.

Cuando se utilice la cadena de filtrado de las reglas para el buzón de correo para identificar el artefacto del ID de ticket, la palabra clave {{object_id}} representa la posición del artefacto del ID de ticket en la cadena de filtrado. Esta palabra clave distingue entre mayúsculas y minúsculas, aunque la regla para el buzón de correo no lo haga.

Ejemplo: uso del artefacto de correo electrónico

El ejemplo siguiente muestra un formato de ARTEFACTO para ser utilizado en una regla para el buzón de correo para un ticket de petición de cambio.

Uso: %REQUEST=@{call_req_id.ref_num}%

Ejemplo: %REQUEST=1234%

Consideraciones de uso del artefacto

Cuando elabora la cadena de filtro de la regla para el buzón de correo, tenga en cuenta lo siguiente:

- Debe existir un límite claro entre el artefacto de ID de ticket y las palabras clave que lo preceden y siguen. Es muy recomendable que incluya texto con espacio en blanco en este texto de límite.
- No termine la parte de la cadena de filtro que precede la palabra clave {{object_id}} en un patrón repetible u opcional que pueda coincidir con el inicio del artefacto de ID de ticket, y no termine un patrón cuya longitud sea ambigua. Por ejemplo, la cadena de filtro no debe contener condición(es|al|amiento)?{{object_id}}, porque esta construcción causa una ambigüedad si un es, al o amiento posterior es el final del texto o parte del prefijo de un ID de ticket desprotegido.

- La parte de la cadena de filtro que sigue a la palabra clave `{{object_id}}` no puede iniciar con un patrón repetible u opcional que pueda coincidir con el final del artefacto de ID de ticket, ni con un patrón cuya longitud sea ambigua, y debe contener por lo menos un elemento de espacio en blanco. Por ejemplo:
 - La cadena de filtro no debe contener `{{object_id}}[A-Z]?`, porque `[A-Z]?` puede coincidir con el último carácter del artefacto de ID de ticket.
 - La cadena de filtro no debe terminar con `{{object_id}}Item`, porque es posible que éste aparezca en el artefacto de ID de ticket, ya sea como sufijo de un ID de ticket en un texto sin formato o artefacto protegido, o como caracteres en un artefacto protegido.
 - El elemento `{{object_id}}` es aceptable, porque el espacio no puede ser parte de un artefacto de ID de ticket y no es parte de un artefacto de ID de ticket protegido o sin formato. Sin embargo `{{object_id}}[\t\r\n]+Item` (paréntesis de apertura, espacio, barra diagonal inversa, t, barra diagonal inversa, r, barra diagonal inversa, n, paréntesis de cierre, signo de más, +Item) es mejor, porque `[\t\r\n]+` compensa el hecho de que el programa de correo inserte un salto de línea después de `{{object_id}}`.
- Cuando elabora las cadenas de filtro para diferentes reglas de buzón de correo, evite utilizar una cadena de filtro que incluya por completo otra cadena de filtro de regla de buzón de correo o en la que la parte anterior o posterior a una palabra clave `{{object_id}}` incluya por completo esa parte de otra cadena de filtro de regla de buzón de correo. Según el orden en que se comprueban estos filtros, una coincidencia de mensajes destinada a un filtro puede coincidir con otro, con una parte del artefacto de ID de ticket que coincide con el texto adicional que distingue entre las dos cadenas de filtro.

Seguridad y protección del artefacto

Los artefactos se utilizan para proteger la entrega de correo en un buzón de correo de las siguientes maneras:

- Use la palabra clave ARTIFACT en notificaciones y frases de notificación.

Nota: El nivel de seguridad del artefacto debe coincidir con la configuración Tipo mínimo de artefacto de la regla para el buzón de correo para el buzón de correo al cual el correo electrónico se envía. Se permiten tipos que son más seguros que lo establecido. Dicho de otra manera, si estableció ARTIFACT=PROTECTED, se permiten tanto PROTECTED como SECURE; no así NONE.

- Establezca la opción Tipo mínimo de artefacto en Detalles de regla para buzón de correo.

Puede incrustar un artefacto en una frase de notificación y especificar el nivel de seguridad para el artefacto, por ejemplo:

`%REQUEST=@{ARTIFACT=PROTECTED:call_req_id.ref_num}%`

Nota: Para obtener más información sobre las tablas para la opción Tipo mínimo de artefacto (`filter_min_artifact_type`) y Detalles de regla para buzón de correo (tabla `usp_mailbox_rule`), consulte la *Guía de referencia técnica*.

Ejemplo: no hay validación de artefactos

El ejemplo siguiente no muestra ningún formato ARTIFACT. No puede realizarse ninguna validación de artefactos.

Uso: `%REQUEST=@{call_req_id.ref_num}%`

Ejemplo: `%REQUEST=1234%`

Ejemplo: no hay validación de artefactos

El ejemplo siguiente muestra el formato `ARTIFACT=NONE`. `ARTIFACT=NONE` equivale a no agregar la palabra clave; no puede realizarse ninguna validación de artefactos.

Uso: `%REQUEST=@{ARTIFACT=NONE:call_req_id.ref_num}%`

Ejemplo: `%REQUEST=1234%`

Ejemplo: validación de un número de ticket en comparación con el hash con fines de confirmación

El ejemplo siguiente muestra el formato `ARTIFACT=PROTECTED`. El formato `PROTECTED` valida un ticket comparándolo con el hash con fines de confirmación. La letra "A" indica el tipo de formato. Las "A" separadas por coma, el código de hash y el número de ticket.

Uso: `%REQUEST=@{ARTIFACT=PROTECTED:call_req_id.ref_num}%`

Ejemplo: `%REQUEST=A,12345678,1234%`

Ejemplo: encriptación del número de ticket

El ejemplo siguiente muestra el formato ARTIFACT=SECURE. El formato SECURE encripta ref_num y luego codifica el resultado en el codificado Base64 para que pueda incluirse con seguridad en el texto del mensaje. La letra "B" indica el tipo de formato. Las "B" separadas por coma y un número de ticket encriptado de contraseña.

Uso: %REQUEST=@{ARTIFACT=SECURE:call_req_id.ref_num}%

Ejemplo:

%REQUEST=B,da1jhr+9U5GVfd2VGH4dsnx2+PaSvygDS2e3IqjptyNSDW2u/K
NPX61nopDu/KB%

Acuerdos de nivel de servicio

Los acuerdos de nivel de servicio o tipos de servicios son acuerdos formalizados entre el centro de servicio al usuario y sus clientes en los que, por lo general, se indica el nivel de servicio que presta el centro de servicio al usuario. En caso de que no se proporcione este nivel de servicio, se penaliza al servicio de asistencia. Por ejemplo, si un servicio de asistencia factura por servicios prestados, puede no recibir el pago completo por el servicio si éste no alcanza el nivel acordado. Por este motivo, la mayoría de los servicios de asistencia se toman muy en serio los acuerdos de nivel de servicio y hacen todo lo posible por cumplir el tipo de servicio especificado en ellos.

Además, casi todos los acuerdos de nivel de servicio registran con gran meticulosidad cuándo se cumplen o infringen dichos acuerdos. Los tipos de servicios definidos en CA Service Desk Manager están diseñados para ayudar al personal del servicio de asistencia a cumplir sus acuerdos de nivel de servicio y a mantener los registros necesarios para confirmar dicho cumplimiento.

Uso de acuerdos de nivel de servicio

En CA Service Desk Manager, los acuerdos de nivel de servicio se configuran por medio de eventos y tipos de servicios para lo siguiente:

- Utilizar eventos para controlar tickets.
- Utilizar tipos de servicio para seguir los compromisos y las programaciones de distribuidores y de la organización a medida que se relacionan a tickets específicos.
- Establecer controles de fecha y hora para el procesamiento de eventos y tipos de servicios.

CA Service Desk Manager permite diseñar y utilizar acuerdos de nivel de servicio de la siguiente manera:

- **Acuerdos de nivel de servicio para varias organizaciones:** puede asignar tipos de servicio diferentes para cada campo de referencia dependiendo de la organización afectada en el ticket. Por ejemplo, el tipo de servicio para un parte de prioridad 1 puede ser distinto para la organización A y para la organización B.
- **Seguimiento de varios acuerdos de nivel de servicio:** los tickets pueden realizar el seguimiento de varios tipos de servicios a la vez con el fin de garantizar la visibilidad de todos los aspectos de un acuerdo de nivel de servicio negociado.
- **Proyecciones de tiempo hasta la infracción:** subsistema que constantemente controla tickets en CA Service Desk Manager y registra cuándo su acuerdo de nivel de servicio entra en infracción basado en su estado actual.
- **Coste de la infracción del acuerdo de nivel de servicio:** el campo Tipo de servicio ayuda con las métricas y con la determinación de la severidad de los tickets abiertos.
- **Tipos de servicio en Tareas:** los tipos de servicio están disponibles en las tareas de workflow.
- **Objetivos del servicio:** los tipos de servicio pueden tener también uno o más objetivos de servicio para medir si el servicio necesario o la reparación se completó dentro del marco de tiempo necesario.

<Procesamiento clásico de acuerdos de nivel de servicio>

En el procesamiento de clásico de acuerdos de nivel de servicio (habilitado si la opción `classic_sla_processing` se instala en el Gestor de opciones) solamente un tipo de servicio se puede aplicar a un ticket en cualquier momento dado. Si los distintos atributos de los partes tienen tipos de servicios diferentes asociados, se emplea el tipo de rango superior de la clasificación. La clasificación de los tipos de servicios se define durante su creación; el valor superior es 1, seguido de 2, y así sucesivamente. Por ejemplo, supongamos que la incidencia tiene un tipo de servicio de resolución en 12 horas (clasificación 2) y se le ha asignado un código de prioridad 1, que tiene un tipo de servicio de resolución en 4 horas (clasificación 1). El tipo de servicio superior determina el comportamiento adoptado para la incidencia asociada. En este ejemplo, la resolución en 4 horas ocupa un puesto superior en la clasificación que la resolución en 12-horas; por ello, se aplica el tipo de servicio de resolución en 4 horas a la incidencia.

Tipos de servicios y eventos

Para realizar el seguimiento de los compromisos y las programaciones tanto de los distribuidores como de las organizaciones en la medida en que se relacionan con determinados partes, es posible adjuntar eventos a los tipos de servicios. Los tipos de servicio ofrecen una manera mucho más flexible y eficaz de adjuntar automáticamente los eventos a los tickets.

Los tipos de servicios admiten de forma automática los acuerdos de nivel de servicio formalizados con los clientes. Gracias a su uso, se puede controlar cualquier aspecto de las situaciones relacionadas con-el momento o las condiciones. Por ejemplo, es posible establecer una póliza que defina un tiempo de resolución para incidencias particulares y asociarle una acción concreta. Los tipos de servicios ofrecen la capacidad de gestionar los proveedores de servicios, los distribuidores y el propio servicio de asistencia de tal modo que se facilita la medición tanto del rendimiento como del cumplimiento.

Los tipos de servicio le permiten hacer lo siguiente:

- Identificar de forma automática el nivel de servicio necesario para partes específicos.
- Identificar las condiciones de infracción del nivel de servicio.
- Enviar de forma automática notificaciones de aviso antes de que venzan los acuerdos de nivel de servicio.
- Configurar los informes de infracción de los acuerdos de nivel de servicio.

Cómo implementar los tipos de servicio

Los tipos de servicio permiten definir acciones basadas en las condiciones definidas por el usuario. Además, se pueden aplicar a los partes. Así, es posible definir un tipo de servicio que especifique un tiempo de resolución para un parte en particular y, después, asociarle un comportamiento que se produzca automáticamente cuando tenga lugar la acción como, por ejemplo, la notificación de una persona del servicio técnico sobre una infracción pendiente. Como los tipos de servicios pueden incluir varios eventos y estos, a su vez, pueden contener varias acciones (para casos verdaderos y falsos), es posible definir un comportamiento más complejo agregando varios eventos a los tipos de servicios.

Para implementar tipos de servicio, realice lo siguiente:

1. Asocie un tipo de servicio con su atributo respectivo. Cabe la posibilidad de definir cuantos tipos de servicios se deseen así como de clasificarlos relacionándolos entre sí.
2. Asigne los tipos de servicios a los elementos de configuración, los contactos, las organizaciones, las categorías de incidencias, las categorías de cambios, las áreas de solicitud y las prioridades. Sólo se puede asignar un tipo de servicio a cada registro.
3. Defina las condiciones específicas que determinen cuándo se cumplen o infringen los acuerdos de nivel de servicio.
4. Identifique las acciones que se deben llevar a cabo para ayudar al servicio de asistencia a cumplir los acuerdos de nivel de servicio.
5. Aplique las acciones oportunas para imponer de manera automática los acuerdos de nivel de servicio.

Ejemplo: asociación de tipos de servicios a contactos

En este ejemplo, se realizan los siguientes pasos para asociar tipos de servicios a contactos:

1. Asigne un tipo de servicio en la página Detalles de contacto.
Cuando se asigna el contacto a un ticket, el campo Tipo de servicio se rellenará de forma automática con el tipo asignado en el registro de contacto.
2. Introduzca Alfa, Beta como nombre en el campo Usuario final afectado de la página Detalles de incidencia y guarde la incidencia.
El campo Tipo de servicio se rellena automáticamente con el valor definido en este registro de contacto. Para sustituir el valor predeterminado, basta con seleccionar otro tipo de servicio.

Tipos de servicio predefinidos

CA Service Desk Manager proporciona tipos de servicio predefinidos. Puede modificar los tipos de servicio predefinidos y crear tipos de servicio que mejor se adapten a las necesidades de su empresa. En CA Service Desk Manager se incluyen varios tipos de servicios predefinidos:

- Resolución en 4 horas
- Resolución en 12 horas
- Resolución en 48 horas
- Resolución en 72 horas

El tipo de servicio de resolución en 4 horas se asocia al código de prioridad 1 cuando se instala por primera vez CA Service Desk Manager, lo que significa que todos los tickets creados con una prioridad 1 se gestionan como si se tuvieran que resolver en las siguientes cuatro horas. Al tipo de servicio de resolución en 4 horas se asocian varios eventos de tipo de servicio con el fin de garantizar una resolución rápida:

- Se notifica a la persona para la que se ha creado el parte que se espera su resolución dentro de las cuatro horas siguientes.
- El gestor de grupo recibe una notificación si no se ha asignado el ticket en los primeros 30 minutos.
- Se envía una notificación de aviso al asignatario y al gestor de grupo si no se ha resuelto el parte en tres horas y media.
- Por último, se envía una notificación de infracción al asignatario y al gestor de grupo si no se ha resuelto el parte en cuatro horas y en éste se establece el indicador de infracción del acuerdo de nivel de servicio.

Ninguno de los demás tipos de servicios predefinidos está asociado a un código de prioridad, pero sí están definidos con eventos parecidos a los descritos para el tipo de resolución en 4 horas. Si lo desea, el administrador del sistema tiene la potestad de asociar estos tipos de servicios a otros códigos de prioridad. Por ejemplo, es posible que desee hacer las siguientes asociaciones:

- Prioridad 2: resolución en 12 horas
- Prioridad 3: resolución en 48 horas
- Prioridad 4: resolución en 72 horas

De forma alternativa, si la asociación que vincula el código de prioridad 1 con el tipo de servicio de resolución en 4 horas no se ajusta a las necesidades, es posible anularla.

las opciones de personalización `cr_sla`, `chg_sla` e `iss_sla` especifican que todas las solicitudes, órdenes de cambio e incidencias deben estar asociadas a algún tipo de servicio. Estas opciones sirven para seleccionar el tipo de servicio más idóneo y aplicarlo a la solicitud, la orden de cambio o la incidencia. Se instalan de manera automática, sin embargo, puede desinstalar o reinstalarlas mediante el Gestor de opciones.

Nota: Para descripciones sobre las opciones de personalización, vea la *ayuda en Línea*. Para obtener información sobre cómo definir tipos de servicio y modificar códigos de prioridad, vea la *ayuda en Línea*.

Configuración de eventos

CA Service Desk Manager emplea condiciones y acciones definidas como eventos para programar y procesar de forma automática los partes y los tipos de servicios, así como realizar su seguimiento, también automático. Cada evento tiene tres características de comportamiento genéricas: condiciones, acciones en caso verdadero y acciones en caso falso. Aparte, se asocia un retardo a las condiciones (y, por lo tanto, a los eventos), que se cuenta desde el momento en el que se guardan los partes. Este retardo determina cuándo se evalúan las condiciones. También cabe la posibilidad de crear eventos automáticos que provoquen acciones específicas cada vez que se producen. Así, por ejemplo, se puede hacer que se genere una notificación automática para las incidencias transferidas con una prioridad " que permanezcan abiertas más de una hora.

- Las *condiciones* identifican el evento para el que se debe preparar CA Service Desk Manager.

Por condición se entiende cualquier estado medible de los partes. Un parte cuyo estado sea Sin asignar es un buen ejemplo de condición. Las condiciones se asocian a acciones, que tienen lugar si la condición es verdadera o, por el contrario, si es falsa. Por ejemplo, el tipo de servicio predefinido de resolución en 12 horas tiene asociado un evento llamado "1 h sin asignar" cuya condición es Incidencia sin asignar. La acción definida para este evento consiste en notificar de la incidencia al gestor del grupo en caso de que la condición sea verdadera con un retardo de una hora. Si una incidencia tiene asignada una resolución en 12 horas, el comportamiento consistiría en "despertar" una hora después de haber guardado el registro, comprobar si continúa sin asignar y, en caso afirmativo, notificar de la incidencia al gestor de grupo.

- Las *acciones* identifican los procesos que se producen automáticamente si la condición es verdadera o falsa tras el período de tiempo especificado.

Puede asignar una sola acción o una lista de acciones que pueden suceder para cada evento supervisado. Cuando se produce un evento que coincide con una condición, CA Service Desk Manager procesa de forma automática las acciones asociadas a la condición. En algunos casos, estas acciones consisten en el procesamiento automático del objeto implicado o bien dan lugar a una notificación.

En la siguiente tabla figuran algunos de los eventos predefinidos para las incidencias. Existen otros eventos predefinidos similares para las solicitudes y las órdenes de cambios, así como otros tantos relacionados con los tipos de servicios predefinidos.

Evento	Descripción
Activa P1: not. incid. a asig.	Notifica al asignatario si la incidencia lleva activa más de 1 hora con prioridad 1.

Evento	Descripción
Activa P2: not. incid. a asig.	Notifica al asignatario si la incidencia lleva activa más de 1 día con prioridad 2.
Sin asignar: transf. de incid.	Transfiere las incidencias si continúan sin asignar durante más de 1 día; notifica al asignatario antiguo, al creador de la incidencia y al nuevo asignatario.

Una vez definidos, estos eventos se pueden adjuntar de manera manual o automática a los tickets y a los tipos de servicios, como sucede con los tipos de servicios predefinidos. Es posible adjuntar varios eventos a cada uno de los tipos de servicios.

Importante: no utilice el Gestor de opciones para instalar eventos automáticos hasta que se creen los eventos. Si se activan estos eventos antes de que estos existan, el rendimiento se ve gravemente afectado. Para obtener más información sobre cómo definir eventos y opciones de evento como `auto_events`, `chg_auto_events` e `iss_auto_events`, vea la [ayuda en línea](#).

Más información:

[Uso del Gestor de opciones](#) (en la página 355)

Objetivos del servicio

Si desea minimizar las infracciones del acuerdo de nivel de servicio, puede crear un conjunto de plantillas de objetivo de servicio para medir cada fase de la resolución de tickets. Como los tipos de servicio, cada objetivo del servicio contiene una condición y estimación del tiempo de finalización. Sin embargo, los objetivos del servicio no proporcionan un mecanismo de acción.

Durante la creación de tickets, un tipo de servicio asigna uno o más objetivos del servicio para seguir cada fase de la resolución de tickets. Cada vez que el ticket cambia, los objetivos del servicio activos evalúan la condición. Si se cumple la condición, el ticket y registro de actividades muestran el tiempo de finalización real. Cuando se supera el tiempo estimado, el ticket muestra la cantidad de tiempo por la que se falló el objetivo.

Los objetivos del servicio permiten hacer lo siguiente:

- verificar que los tickets del mismo tipo de servicio siguen los mismos objetivos del servicio.
- controlar si se cierran los tickets en los marcos de tiempo necesarios.
- ver información como el número restante de minutos antes de que se complete un objetivo del servicio.

La configuración de objetivos del servicio es un proceso que consta de dos pasos. Primero, puede crear un conjunto de plantillas de objetivo de servicio. A continuación, puede vincular las plantillas con un tipo de servicio concreto. En el momento de la creación de tickets, la plantilla apropiada se adjunta automáticamente al ticket en función del tipo de servicio.

Al crear plantillas de objetivo de servicio, tenga en cuenta lo siguiente:

- Considere el resultado obligatorio para cumplir el objetivo del servicio. Utilice una condición existente o una macro de condición definida por el sitio para evaluar los datos del ticket. Si es necesario, personalice o escriba una nueva macro para gestionar el objetivo del servicio.
- Calcule los costes del incumplimiento y la sanción previstos en función de los Acuerdos de nivel de servicio.
- Asigne por lo menos una plantilla de objetivo de servicio a un tipo de servicio.

Procedimiento para crear una plantilla de objetivo de servicio

1. Cree una plantilla de objetivo de servicio para gestionar solicitudes, incidentes, problemas, órdenes de cambio o incidencias.
2. Vincule la plantilla de objetivo de servicio con un tipo de servicio.
3. Asigne los detalles de la plantilla de objetivo de servicio a una categoría de ticket como tickets de solicitud, incidente, problema, orden de cambio o incidencia.

Cada vez que un usuario crea un ticket, el estado del objetivo del servicio aparece automáticamente en la ficha Tipo de servicio.

Contratos de servicio

El modelo de acuerdo de nivel de servicio incluye el contrato de servicio. El contrato de servicio define las condiciones del acuerdo de nivel de servicio para una organización en particular, incluidos sus Tipos de servicios, Áreas de solicitud y Categorías de incidencias o cambios. Estas definiciones hacen referencia a categorías *privadas* y tipos de servicios *privados*.

Nota: Las categorías y los tipos de servicio *privados* sólo se pueden emplear en los tickets en los que esté vigente el contrato de servicio pertinente.

El contrato de servicio aplicable a cada parte se determina según la *organización afectada* del parte, que coincide siempre con la organización del usuario final afectado que figura en el parte (campo Organización de los registros de contactos). Para el ticket, sólo se pueden elegir las áreas o las categorías incluidas en los contratos de servicio. Además, los únicos tipos de servicios que se pueden aplicar son los *privados* que figuran en el contrato. De este modo, se garantiza que no se mezclen por accidente los acuerdos de nivel del servicio de unas organizaciones con los de otras.

Por otro lado, los contratos de servicio asignan los tipos de servicios a campos de referencia comunes de los partes, como Prioridad y Activo. Esta asignación asocia tipos de servicio con los atributos de un ticket. Por ejemplo, si el contrato de una organización puede asignar tipos de servicios a cada uno de los cinco objetos de prioridad, cada vez que se crea un parte con una determinada prioridad, se aplica el tipo de servicio asignado.

Las categorías y los tipos de servicios pueden definirse fuera de los contratos y se consideran *públicos*. Las definiciones públicas se emplean cuando los tickets carecen de un contrato de servicio en vigor. La falta de un contrato de servicio puede ocurrir si el usuario final no tiene organización, o el contrato de la organización está inactivo. Una definición pública es una copia de seguridad útil o el mecanismo predeterminado. Los tipos de servicios públicos se definen directamente en las categorías y en otros objetos de campos de referencia.

Todos los tipos de servicio aplicables se asignan al ticket. Así se garantizan la visibilidad y el cumplimiento de todos los aspectos de los acuerdos de nivel del servicio.

- Una impresora puede tener un tipo de servicio que exige la presencia de un técnico en menos de dos días
- El tipo de servicio de un objeto de prioridad puede exigir la devolución de la llamada en menos de una hora.

Al aplicar ambos tipos de servicios, se impone el cumplimiento de estas acciones obligatorias.

El seguimiento de varios tipos de servicios también ayuda a priorizar los partes. Supongamos, por ejemplo, que a un parte relacionado con un teclado estropeado se le asigna un tipo de servicio de prioridad baja. Sin embargo, si el usuario final afectado necesita urgentemente el teclado, la prioridad de servicio se puede aumentar.

Nota: El modelo de acuerdo de nivel de servicio se impone de forma predeterminada. En las versiones anteriores de CA Service Desk Manager, sólo se aplicaba un único tipo de servicio a cada parte. La elección del tipo de servicio implicaba la búsqueda del tipo de mayor *rango* de todos los tipos de servicios posibles. Un modelo que utiliza el esquema de clasificación se puede utilizar mediante la instalación la opción 'classic_sla_processing'.

Migración de contratos de servicio

Si se instala CA Service Desk Manager a partir de una migración, se activa de forma predeterminada la opción `classic_sla_processing` con objeto de que el procesamiento de acuerdos de nivel de servicio continúe como hasta después de la migración. Esta continuación le otorga tiempo para crear contratos de servicio apropiados y después de lo cual se desactiva `classic_sla_processing`.

Al elaborar los contratos de servicio, no hace falta crear tipos de servicios, áreas de solicitud ni categorías, sino que se puede usar el botón Copiar de la ventana Detalles de contrato de servicio para copiar los objetos existentes en los nuevos contratos.

En caso de que en la instalación anterior esté marcado el campo `support_lev` como obligatorio para todos los tipos de parte, es preciso eliminar esta restricción. Aunque el campo `support_lev` sigue existiendo, no se define en el modelo actual por lo que se produciría un error de campo obligatorio en los nuevos tickets. Esto afecta a los objetos de solicitud (cr), incidencia (iss) y orden de cambios (chg).

Hora de infracción

Con el nuevo modelo de acuerdos de nivel de servicio en uso, el sistema de hora de infracción de CA Service Desk Manager ayuda a realizar el seguimiento y la priorización de tickets de acuerdo con la hora de incumplimiento previsto. Este sistema supervisa todos los partes activos y define la hora de incumplimiento previsto para cada uno de los tipos de servicios. Puede informar y clasificar los tickets según el momento y el coste de la infracción, lo que ayuda a resolver las incidencias más urgentes y costosas en primer lugar.

El sistema de hora de infracción controla todos los tickets activos y evalúa sin intervención del usuario los eventos del acuerdo de nivel de servicio para determinar cuáles de ellos establecerán el indicador de infracción del acuerdo. En realidad, los eventos no se ejecutan; el sistema se limita a contemplar el resultado de cada evento basándose en el estado actual de los tickets. Si la evaluación da como resultado una acción que establece el indicador de infracción del acuerdo de nivel de servicio, se actualiza el tipo de servicio adjunto al ticket con un valor de hora de infracción. Este valor se compone de la fecha y la hora cuando se inicia el evento que define la infracción del acuerdo.

La evaluación se lleva a cabo cada vez que se insertan o se actualizan partes. Dado que a menudo se actualizan tickets en la rápida sucesión, la evaluación se retrasa durante un periodo corto. El intervalo de retardo se controla por medio de la opción `ttv_evaluation_delay`. Cuando transcurre el plazo de retardo, el sistema de hora de infracción evalúa todos los eventos del acuerdo de nivel de servicio que puedan establecer el indicador de infracción del acuerdo.

Todos los eventos cuentan con una condición opcional y un conjunto de acciones (macros) cuyo inicio depende del resultado de la condición. Para garantizar un rendimiento adecuado, el sistema de hora de infracción almacena en caché la información de las plantillas de eventos, que se actualiza cada cierto tiempo. Las proyecciones de este sistema que tengan que ver con las plantillas de eventos recién actualizadas pueden ser inexactas durante varios minutos.

Nota: Las proyecciones de hora de infracción aparecen en la ficha Tipo de servicio de todos los tickets. El sistema de hora de infracción se activa mediante la opción `ttv_enabled`.

Zonas horarias y turnos

Con el fin de satisfacer las exigentes demandas empresariales en cuanto a la ejecución automatizada de las aplicaciones, CA Service Desk Manager permite definir todas las zonas horarias y los turnos que desea y registrarlos para facilitar la consulta.

- Las zonas horarias identifican la zona donde se ubican los usuarios, los elementos de configuración, etc.
- Los turnos definen el período durante el cual tienen vigencia la supervisión de eventos, las horas laborables de los tipos de servicios o los acuerdos de nivel de servicio.

La capacidad de determinar la línea de actuación adecuada en función de cuándo se producen los eventos puede llegar a ser básica para la correcta gestión de los eventos. Todas las funciones de CA Service Desk Manager pueden emplear los husos horarios y los turnos que se definan.

Configuración de la zona horaria

Los códigos de zona horaria definen la zona horaria desde la que los usuarios suelen acceder al sistema (es decir, la hora local del usuario) o la zona en la que se encuentran ubicados los elementos de configuración. Las horas laborables se indican siempre en el huso horario del servidor de CA Service Desk Manager. Esto significa que siempre cabe la posibilidad de comparar de manera uniforme las horas laborables.

Los husos horarios se emplean para gestionar los tipos de servicios, las elevaciones a instancias superiores y la respuesta general a los usuarios finales afectados en función de la capacidad de CA Service Desk Manager para presentar la hora correcta en cada huso. CA Service Desk Manager ajusta de forma automática la diferencia entre las zonas desde donde inician la sesión los usuarios o donde se hallan los elementos de configuración y la zona horaria donde se ejecuta el servidor. Los husos horarios adoptan el formato de la hora del meridiano de Greenwich (GMT).

Nota: Para obtener más información sobre cómo definir las zonas horarias, consulte la *ayuda en línea*.

Cómo gestionar varias zonas horarias para tipos de servicio

Los usuarios y servidores de CA Service Desk Manager se pueden encontrar en distintas zonas horarias. La diferencia horaria puede hacer que los usuarios pierdan horas y fechas de caducidad del tipo de servicio.

Para corregir la diferencia horaria, puede configurar CA Service Desk Manager para que muestre las horas de vencimiento del tipo de servicio en la zona horaria del usuario de final. Si dos usuarios en distintas zonas horarias ven el mismo ticket, cada uno verá valores de hora de vencimiento según la zona horaria del equipo local. Sin embargo, los valores de hora de inicio siempre reflejarán la zona horaria del servidor.

Para configurar la zona horaria del usuario final, realice lo siguiente:

1. Cree un código de servidor que identifique el nombre de servidor y la zona horaria.
2. Cree o actualice un tipo de servicio. Establezca el campo Utilizar zona horaria de usuario final en Sí.

Un valor de Sí hace que la hora de vencimiento se muestre y se actualice según la zona horaria de cada usuario.

Ejemplo: cómo mostrar las fechas de caducidad del tipo de servicio en la zona horaria de cualquier usuario

En este ejemplo, puede configurar CA Service Desk Manager para mostrar fechas de caducidad de tipo de servicio en la zona horaria de cualquier usuario. El servidor y el usuario están en equipos distintos en zonas horarias diferentes.

Procedimiento para crear un código de servidor que identifique el nombre de servidor y la zona horaria

1. En la ficha Administración del servidor host, seleccione Service Desk, Código de aplicación.
2. Haga clic en Códigos, Servidores.
Se muestra la lista de servidores.
3. Haga clic en el servidor host local.
Aparecerá la página Detalles de nombre del servidor.
4. Defina la zona horaria. Por ejemplo, establezca la zona horaria a GMT (UE). El nombre de host local debe coincidir con el valor NX_LOCAL_HOST almacenado en NX.env para el servidor.
5. Haga clic en Guardar.

El servidor host utiliza la nueva zona horaria. Cuando el usuario ve un ticket, la hora de inicio reflejará la zona horaria del servidor.

Procedimiento para crear un tipo de servicio

1. En la ficha Administración, seleccione Tipos de servicio.
Aparecerá la lista de tipos de servicio.
2. Haga clic en Resolución de prioridad 1 u otro tipo de servicio que gestione solicitudes de prioridad 1.
Se muestra la página Actualizar tipo de servicio.
3. Active la casilla de verificación Utilizar zona horaria de usuario final.
4. Haga clic en Guardar.
El registro del tipo de servicio se actualiza.

Procedimiento para ver las zonas horarias en el ticket

1. En otro equipo, abra un ticket de solicitud y establezca la prioridad en 1.
Nota: Si está utilizando Objetivos del servicio, establezca los valores en el ticket para hacer que el objetivo utilice Resolución de prioridad 1.
2. Vea el ticket y haga clic en la ficha Tipo de servicio.
La hora de inicio reflejará la zona horaria del servidor. La hora de vencimiento reflejará la hora del equipo local del usuario final.
3. Cierre la página que muestra el ticket de solicitud.
4. Cambie la zona horaria en el equipo local del usuario final.
5. Vea el tipo de servicio del ticket en el equipo local del usuario final para ver los valores de hora de vencimiento correspondientes en función de la zona horaria del usuario.
La hora de vencimiento reflejará la nueva zona horaria.

Nota: Para obtener información detallada sobre tipos de servidor o código de servidor, consulte la *Ayuda en línea*.

Configuración de turnos

Los turnos identifican los días, las fechas y las horas en los que se encuentran vigentes los eventos o las programaciones. Puede especificar los días o las fechas, o ambas cosas. La especificación de las horas es opcional.

Nota: Para obtener más información sobre la definición de turnos, consulte la *ayuda en línea*.

Cuando se supervisan eventos en relación con los partes, los turnos definen cuándo se supervisan dichos eventos, es decir, cuándo empieza a contar el tiempo. Por ejemplo, al emplear el evento predefinido Activa P1: not. incid. a asig., si se abre una incidencia de prioridad 1 a las 4:45 p. m. y la programación de turnos va de las 9:00 a. m. a las 5:00 p. m., el evento supervisado envía la notificación automática pertinente al asignatario de la incidencia a las 9:45 a. m. del día siguiente.

Nota: Los turnos se emplean para asignar los tickets a los contactos de forma automática.

Más información:

[Establecimiento de la estructura de soporte - CA](#) (en la página 267)

Seguridad

Antes de permitir el uso de CA Service Desk Manager, es importante que configure la seguridad para determinar lo siguiente:

- qué usuarios pueden acceder al sistema.
- qué nivel o niveles de acceso pueden tener los usuarios.
- cómo se autentican los usuarios al iniciar sesión.

Nota: Para obtener detalles sobre cómo lograr tareas de administración de seguridad, consulte la *ayuda en Línea*.

Configuraciones de la base de usuarios de CA EEM y CA Workflow

CA EEM es un repositorio central que contiene información de usuarios (identidades). CA EEM define la autenticación de usuario y el acceso a otras aplicaciones. Si existen varios productos de CA instalados, es posible que algunos de ellos se sirvan de CA EEM para almacenar las identidades y acceder a las políticas. CA Service Desk Manager solamente utiliza CA EEM para la autenticación. CA EEM no es una opción de configuración de CA Service Desk Manager y debe ser instalado por separado.

El repositorio de CA EEM de registros de usuarios es *una* de las dos siguientes fuentes:

- Un directorio LDAP externo
- Sus propias tablas internas de MDB

CA EEM dispone de una interfaz LDAP propia cuando se configura su uso con MDB.

Nota: Las tablas de MDB utilizadas por CA EEM son diferentes de las utilizadas por CA Service Desk Manager.

Si su organización utiliza un servidor de directorios, como Active Directory o eTrust Directory, considere la posibilidad de configurar CA EEM de modo que utilice el directorio para su base de usuarios. Esta configuración hace que se pueda acceder a los usuarios de su directorio desde cualquier otra aplicación que utilice CA EEM. Como CA EEM centraliza la gestión del acceso, se suele instalar en un solo servidor.

Nota: Para obtener más información sobre la instalación, consulte la *Guía de implementación*.

CA Workflow

Durante la instalación de CA Service Desk Manager, puede instalar opcionalmente CA Workflow, un motor de workflow incrustado. CA Workflow se sirve de CA EEM para toda la información de usuario, por ello, CA EEM gestiona todos los intentos de autenticación y determinados permisos. CA Workflow desconoce los registros de contacto de CA Service Desk Manager.

Nota: Para obtener información sobre la configuración del acceso a CA Workflow, consulte la *Guía de implementación*.

CA Service Desk Manager

CA Service Desk Manager almacena la información de los contactos en tablas de MDB. Estas tablas no tienen ninguna relación con CA EEM. CA Service Desk Manager prescinde de CA EEM para la gestión del acceso y las identidades. CA Service Desk Manager gestiona sus propias opciones de acceso y seguridad mediante tipos de acceso y particiones de datos.

CA Service Desk Manager solamente utiliza CA EEM para la autenticación. Si desea utilizar CA EEM para autenticar los usuarios en CA Service Desk Manager, instale CA EEM. Si integra CA Service Desk Manager con CA EEM, reemplaza la autenticación de sistema operativo de CA Service Desk Manager con autenticación de CA EEM.

Nota: Para obtener información sobre la instalación de CA EEM, consulte la *Guía de implementación*. Para integrar CA EEM y CA Service Desk Manager, debe establecer las opciones *eiam_hostname*, *use_eiam_artifact* y *use_eiam_authentication* en Gestor de opciones, Seguridad. Para obtener más información sobre estas opciones, consulte la *ayuda en línea*.

La base de usuario de CA Service Desk Manager está separada de la de CA EEM y, por lo tanto, se separa de la base de usuario de CA Workflow. La ventaja de CA Workflow es que los elementos del workflow se pueden asignar para su realización a personas que se encuentren fuera del ámbito de CA Service Desk Manager. Esto resulta de gran utilidad cuando CA EEM señala al servidor LDAP de la organización.

El reto está en la integración de CA Service Desk Manager. Un elemento de trabajo no se puede asignar directamente al registro de contacto de CA Service Desk Manager real. Se puede hacer la asignación del elemento de trabajo a los contactos de CA Service Desk Manager solamente si se cumplen las dos condiciones siguientes:

- El contacto de CA Service Desk Manager tiene un registro correspondiente en CA EEM
- Esos registros tienen ID de usuario coincidentes

En resumen:

- CA Service Desk Manager utiliza MDB para almacenar la información de los contactos. CA Service Desk Manager también se caracteriza por la integración de LDAP, que le permite crear contactos desde servidores LDAP y sincronizar los contactos existentes con el directorio.
- CA EEM es la solución de CA para la gestión centralizada de usuarios. Si existen varios productos de CA instalados, es posible que usen CA EEM para almacenar las identidades y acceder a las pólizas.

- CA EEM se puede configurar para señalar a un directorio externo (LDAP) o utilizar la MDB para almacenar información sobre el usuario. CA EEM dispone de una interfaz LDAP propia si se configura su uso con la MDB.

Nota: Las tablas que utiliza CA EEM en la MDB son diferentes de las que utiliza CA Service Desk Manager.

- CA Workflow siempre utiliza CA EEM para la información de usuario y la autenticación. Los elementos de trabajo sólo se pueden asignar a usuarios que conozca CA EEM y sólo los usuarios que defina CA EEM pueden acceder al recurso IDE y a la interfaz Web de lista de trabajo de CA Workflow.

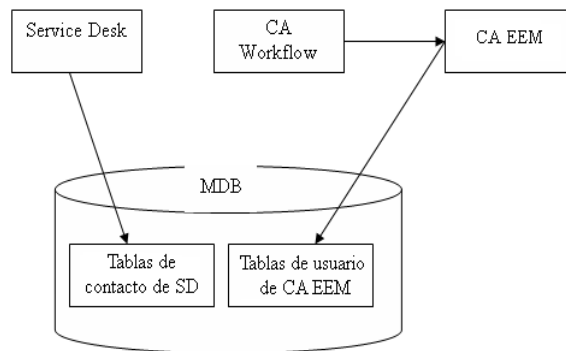
En los temas siguientes se abordan las diversas opciones de configuración para los productos y se explica el modo en el que influyen en la integración de CA Service Desk Manager y CA Workflow. Seleccione la configuración que mejor coincida con su uso de CA Workflow y (de forma opcional) un servidor de directorio LDAP.

Configuración predeterminada

CA Service Desk Manager y CA Workflow almacenan información de usuario después de una instalación predeterminada del siguiente modo:

- CA Service Desk Manager almacena información de usuario en las tablas de contacto de CA Service Desk Manager en la MDB.
- CA Workflow utiliza a CA EEM para almacenar información de usuario en las tablas de usuario de CA EEM en la MDB.

El diagrama siguiente ilustra donde los productos almacenan información de usuario:

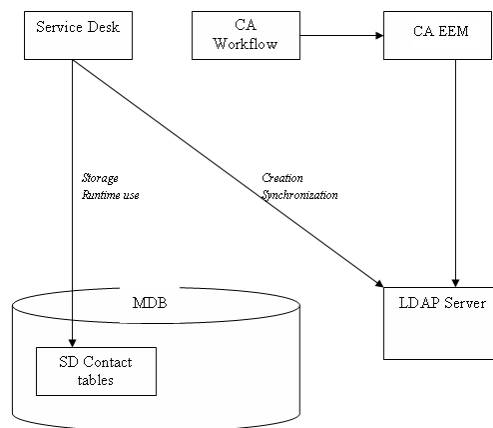


Considere utilizar la configuración predeterminada si su sitio hace poco o ningún uso de CA Workflow o un servidor de directorio de LDAP. Esta configuración puede presentar algunos retos. Cada usuario de CA Workflow requiere un registro de usuarios de CA EEM.

Configuración del servidor LDAP externo

La administración de contactos es más sencilla si CA Service Desk Manager y CA Workflow utilizan el mismo servidor de directorio LDAP. Esta configuración tiene especial utilidad si ya se usa en el sitio un servidor LDAP como directorio principal para los usuarios. Con la ayuda de las capacidades LDAP de CA Service Desk Manager, los ID de usuario de los registros de contacto coinciden con las existentes en el directorio, lo que facilita la asignación de elementos de trabajo a los analistas de CA Service Desk Manager. La integración es aún más sencilla si CA Service Desk Manager emplea CA EEM para la autenticación.

El diagrama siguiente muestra un escenario en el cual todos los usuarios en el directorio LDAP automáticamente tienen acceso a aplicación Web de lista de trabajos de CA Workflow. Aunque CA Service Desk Manager sigue utilizando las tablas de contactos de MDB para sus registros de usuarios, estos pueden importarse de los registros del servidor LDAP y sincronizarse con ellos en forma periódica.

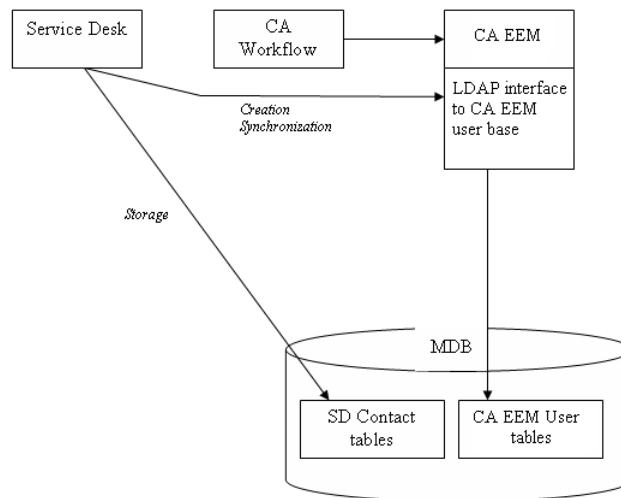


Más información:

[Datos del directorio LDAP](#) (en la página 206)

CA EEM como configuración de LDAP

Cuando se configura CA EEM para utilizar la MDB en lugar de un directorio externo con el objetivo de almacenar información del usuario, CA EEM expone el directorio de usuario mediante una interfaz LDAP. Si el sitio no usa el servidor LDAP externo, puede aprovechar las ventajas de la configuración de CA Service Desk Manager externa al configurar CA Service Desk Manager para que use CA EEM como origen LDAP. Esta configuración puede ser útil si el sitio no emplea ningún servidor LDAP, pero desea consolidar la gestión de los usuarios en CA EEM. Otros productos de CA también utilizan CA EEM, que puede simplificar la gestión del usuario en gran medida.



Nota: Esta configuración sólo se aplica cuando CA EEM está configurado para utilizar MDB. Si CA EEM está configurado en un servidor LDAP externo, configure CA Service Desk Manager para que señale al mismo servidor LDAP, *no* a CA EEM.

Mejorar

Si se migra de una versión anterior de CA Service Desk Manager o se cargan por lotes muchos registros de contactos, debe agregar estos usuarios en forma manual a CA EEM para proporcionarles acceso a CA Workflow.

Gestión de usuarios en CA EEM

La información siguiente analiza las diversas opciones de gestión de los usuarios en CA EEM.

Configuración del almacenamiento de usuarios de CA EEM

Puede configurar CA EEM para almacenar registros de usuarios en un directorio LDAP externo o en sus propias tablas de MDB internas. Cuando CA EEM usa un directorio LDAP externo, es una interfaz de sólo lectura, no puede agregar ni modificar usuarios en la interfaz de CA EEM.

Procedimiento para configurar el origen de los registros de usuarios de CA EEM

1. Haga clic en Inicio, Programas, CA, eTrust, eTrust Embedded IAM, IU de Embedded IAM.

Aparecerá la interfaz de usuario de CA EEM.

2. Haga clic en la ficha Configurar.
3. Haga clic en la subficha Servidor de Embedded IAM.
4. En el panel izquierdo, haga clic en el vínculo Usuarios globales/Grupos globales.
5. En el panel derecho, seleccione una de las opciones siguientes:
 - Guardar en la base de datos de administración de CA (CA-MDB)
 - Referencia desde un directorio externo

Nota: Si selecciona la referencia de una opción de directorio externo, se le solicita los detalles del servidor LDAP.

6. Haga clic en Guardar.

De este modo termina la configuración del almacenamiento de usuarios de CA EEM.

Nota: Para obtener más información sobre CA EEM, consulte la *ayuda en línea de CA EEM*.

Cómo agregar usuarios y grupos

Si CA EEM está configurado para hacer referencia a un directorio externo, no puede agregar usuarios con la interfaz de usuario de CA EEM. CA EEM es una interfaz de sólo lectura del servidor LDAP. Para actualizar los registros de los usuarios, es preciso emplear la interfaz suministrada con el producto de servidor LDAP en particular del que se disponga.

Procedimiento para agregar un nuevo registro de usuario:

1. Haga clic en Inicio, Programas, CA, eTrust, eTrust Embedded IAM, IU de Embedded IAM.
2. Conéctese con el nombre de usuario y la contraseña de administrador de CA EEM. Estos se especifican durante la instalación de CA EEM. Se debe instalar CA EEM en forma separada y no es una opción de configuración de CA Service Desk Manager.
3. Haga clic en la ficha Gestionar identidades.
4. En el panel izquierdo haga clic en la ficha Usuarios para buscar y actualizar registros de usuarios existentes.

Nota: Para gestionar los grupos de CA EEM, haga clic en la ficha Grupos.

5. Haga clic en el icono que aparece a la izquierda de la carpeta Usuarios. Aparecerá el formulario para crear un registro de usuario.
6. Complete el formulario y haga clic en Guardar.

El nuevo registro de usuarios de CA EEM se guardó en la MDB.

Nota: Los pasos para editar un registro de usuarios existente y para conservar los registros de grupos son similares a estos pasos. Para obtener información, consulte la *ayuda en línea de CA EEM*.

Configuración del acceso de CA Workflow en CA EEM

CA EEM se encarga de autenticar todos los inicios de sesión en CA Workflow. Para acceder a la aplicación de la lista de trabajos o IDE de CA Workflow, la persona debe tener un registro de usuario de CA EEM. El administrador de CA Workflow, que se especifica durante la configuración de CA Service Desk Manager, tiene acceso completo.

De forma predeterminada, CA Service Desk Manager utiliza a este usuario para la integración de Workflow. Esta cuenta se define con las opciones cawf_username y cawf_password en el gestor de opciones. Es necesario asegurarse de que el nombre de usuario y la contraseña indicados en estas opciones sean correctos y de que el usuario dispone de acceso completo a los recursos de CA Workflow de CA EEM.

CA Workflow también emplea CA EEM para restringir el acceso a determinadas funciones de CA Workflow. Este acceso está controlado por dos clases de recursos denominados IDE y Process.

- El recurso IDE dispone de una única acción llamada *login*, que ofrece acceso de inicio de sesión al recurso IDE. Los usuarios deben tener permiso para esta acción y poder iniciar sesión en la aplicación IDE de CA Workflow.
- El recurso Process dispone de una sola acción llamada *start*, que permite iniciar instancias de procesos. Los usuarios deben tener permiso para esta acción para poder iniciar procesos en la aplicación Web de lista de trabajo.

Nota: Todos los usuarios que CA EEM conoce pueden acceder a la aplicación de lista de trabajos de CA Workflow para ver y realizar tareas de elementos de trabajo. Este permiso sólo está disponible para iniciar nuevas instancias desde la lista de trabajos. Estas clases de recursos se definen en CA EEM con la instancia de aplicación de CA Service Desk Manager. Al iniciar sesión en la interfaz de usuario Web de CA EEM, debe especificar la instancia de aplicación de CA Service Desk Manager para poder ver los recursos, las pólizas y los grupos aquí analizados.

Si los usuarios necesitan iniciar una sesión en el recurso IDE o iniciar instancias de procesos, precisan que se les autorice el acceso a los recursos y a las acciones antes mencionados. En el proceso de configuración de CA Service Desk Manager se agregan dos políticas a CA EEM que sirven para otorgar el acceso a dichos recursos. Por comodidad, las políticas otorgan acceso a dos grupos en su instancia de aplicación: administradores de workflow e iniciadores de procesos de workflow. Si se desea que otros usuarios obtengan acceso al recurso IDE, basta con agregarlos al grupo de administradores de flujos de trabajo. Al agregar usuarios al grupo Iniciadores de procesos de workflow les permite iniciar procesos desde la aplicación Lista de trabajos.

Procedimiento para agregar usuarios a los grupos anteriores o eliminarlos de ellos

1. Inicie sesión en la interfaz Web de CA EEM
2. En la página de inicio de sesión, seleccione la aplicación CA Service Desk Manager y especifique el nombre y la contraseña de administrador de CA EEM.
3. En la página principal de CA EEM, seleccione Gestionar identidades.
4. Acceda a la función de búsqueda de la ficha Users, escriba los criterios oportunos y ejecute la búsqueda.

5. Seleccione un usuario en la lista de resultados.
6. En la pantalla de detalles del usuario, agregue nuevos miembros a otros grupos o elimine los existentes en la sección Application Group Membership.

Nota: Si no aparece esta sección, quizá deba hacer clic en el botón Add Application User Details.

7. Cuando termine, haga clic en Guardar.

Se agrega el usuario o se elimina, según se haya elegido.

Asignación de elementos de trabajo de CA Workflow

El rol de los elementos de trabajo de CA Workflow se puede asignar a actores humanos y no humanos. Ejemplos de estos últimos son objetos Java personalizados, procesos de la línea de comandos u otras instancias de procesos de CA Workflow. En el caso de los actores humanos, el rol del elemento de trabajo se define en la lista de usuarios globales, que es el repositorio de usuarios de CA EEM. Se trata de una lista de ID de los usuarios separados por punto y coma. Por ejemplo:

ServiceDesk; abeju01; Mi grupo

Esta serie asignaría el elemento de trabajo a usuarios de ServiceDesk, abeju01 y a cualquiera que pertenezca a Mi grupo. Eso significa que cualquiera de ellos se puede encargar de realizar el elemento de trabajo.

Nota: Todos los usuarios y grupos deben ser conocidos para CA EEM, por lo que se entiende que el grupo Mi grupo es un grupo de CA EEM, no de CA Service Desk Manager.

Para asignar los elementos de trabajo de forma dinámica a un único usuario, es necesario definir la lista de usuarios de roles en el valor \$MiUsuario.

Nota: NO incluya la cadena entre comillas dobles.

Declare un atributo de cadena llamado MiUsuario en la definición del proceso. Al crear el elemento de trabajo oportuno, se utiliza para su asignación el valor que contenga MiUsuario. Por lo tanto, se debe asignar un valor válido a MiUsuario, ya sea el nombre de un usuario o una lista de nombres de usuario separados por punto y coma. Es obligatorio efectuar esta asignación antes de usarlo en cualquier elemento de trabajo.

La demostración de la definición de pedidos de equipos incluye un ejemplo de asignación de ID de usuarios a las variables. Se supone que el ID de usuario de un registro de contacto de CA Service Desk Manager coincide con el ID de usuario del registro de usuario correspondiente de CA EEM. En esta demostración se explica el modo de recuperar ID de usuario de CA Service Desk Manager con la interfaz del servicio Web. Estos ID de usuario pueden proceder del parte en cuestión (como el asignatario, el asignatario de la categoría, etc.).

Procedimiento para resumir la definición de la asignación de elementos de trabajo

1. Inicie IDE de CA Workflow.
2. Haga doble clic en el nombre de la definición del proceso que desee editar.
La definición de proceso aparece en la ventana Diseñador de procesos.
3. Acceda a la ficha Roles.
4. Agregue o actualice un rol.
5. Seleccione Lista de usuario global de la lista de Actores disponibles y haga clic en Editar.
6. Escriba una lista de ID de usuario de CA EEM separados por punto y coma. Si lo desea, haga clic en el botón Examinar para buscar y seleccionar usuarios que CA EEM conoce.

Consideraciones sobre seguridad

Al instalar CA Service Desk Manager por primera vez, el sistema está configurado para permitir el acceso máximo a cualquier contacto para el que no se haya definido ningún tipo de acceso definido en el registro del contacto. Es posible que desee hacer modificaciones adicionales a la implementación de seguridad predefinida. Como mínimo, debería ejecutar los pasos siguientes antes de permitir que se empiece a trabajar con la aplicación:

1. Repase los tipos de acceso predefinidos para determinar un valor predeterminado razonable para el sistema.

El administrador se establece como el tipo de acceso predeterminado, aunque no suele ser una elección adecuada en la mayoría de sitios. Por ejemplo, algunos sitios ofrecen acceso a CA de sólo lectura a la mayoría de los miembros de la organización de IT. Si establece el usuario CMDB como el tipo de acceso predeterminado, no tendrá que configurar el tipo de acceso de los nuevos usuarios salvo que necesiten privilegios adicionales. De igual forma, si la mayoría de los usuarios requieren el privilegio de escribir información de configuración, puede seleccionar Analista de CMDB como el tipo de acceso predeterminado.

2. Asigne explícitamente los tipos de acceso del resto de contactos.

Por ejemplo, si elige Usuario de CMDB como el tipo de acceso predeterminado, modifique los registros de contactos de los contactos de analistas para asignar el tipo de acceso de analista.

Nota: Para obtener más información, consulte la *ayuda en línea*.

Autenticación de CA EEM para CA IT PAM

CA Service Desk Manager y CA IT PAM se comunican mediante un intercambio de servicios Web por HTTP. Aunque todas las medidas están hechas para que pase la mínima cantidad de información confidencial entre los productos, una entidad maliciosa puede acceder a nombres de usuario, contraseñas e información propietaria. Puede tomar pasos deliberados para proteger la comunicación del servidor.

En el caso de la autenticación de CA IT PAM, tenga en cuenta las siguientes recomendaciones:

- Una opción es configurar CA IT PAM para utilizar CA EEM como servidor de autenticación. CA IT PAM implementa políticas y grupos predeterminados dentro de CA EEM. Puede modificar las políticas y grupos predeterminados para cubrir las necesidades de su organización.
- El uso de CA EEM elimina la necesidad de introducir nombres de usuario y contraseñas de texto sin formato con fines de autenticación. Si utiliza multicliente, se requiere CA EEM para habilitar el multicliente en CA IT PAM.

Nota: Para lograr seguridad de autenticación en esta integración, no es necesario que CA Service Desk Manager esté configurado para utilizar CA EEM. Sin embargo, se requiere CA EEM para la implementación de multicliente de CA IT PAM. Para obtener información sobre la implementación de multicliente con CA IT PAM, consulte la documentación de guía del usuario de CA IT PAM. Si desea obtener información sobre cómo configurar CA IT PAM para utilizar CA EEM como servidor de autenticación, consulte la documentación de configuración e instalación de CA IT PAM.

- Configure CA IT PAM para comunicarse a través de comunicaciones seguras en HTTPS. Las URL HTTPS utilizan SSL/TLS para eliminar intercambios de texto sin formato mientras protegen datos confidenciales y con derecho de propiedad de divulgación maliciosa o accidental.

Nota: Para obtener información sobre cómo configurar CA IT PAM para utilizar HTTPS, vea la documentación de configuración e instalación de CA IT PAM.

Autenticación de usuarios

CA Service Desk Manager proporciona una solución para la autenticación de usuarios que es posible personalizar como parte del tipo de acceso. Todas las interfaces de CA Service Desk Manager, así como otros productos de CA, emplean el mismo tipo de autenticación.

Nota: Si le resulta más adecuado, cabe la posibilidad de configurar la autenticación de los usuarios de CA Service Desk Manager en un equipo independiente. Para obtener más información, consulte la *Guía de implementación*.

El proceso de autenticación es flexible, lo que permite el aprovechamiento de otros mecanismos de autenticación externos, como el de Windows, la validación de usuarios HTTPD o la autenticación LDAP. También puede utilizar diversas opciones de autenticación interna, como el uso de contraseñas en el sistema operativo, los números PIN, el acceso de usuario como invitado o la denegación absoluta del acceso.

Cómo realiza CA Service Desk Manager la autenticación de usuarios

CA Service Desk Manager autentica a los usuarios basándose en el ID de usuario que se haya definido en sus registros de contacto. El producto también hace lo siguiente cuando un usuario solicita acceso al sistema:

1. Si algún ID de usuario externo está disponibles (de la validación HTTPD o en Windows), CA Service Desk Manager busca el contacto pertinente por ID de inicio de sesión. Si, al encontrar el contacto, se comprueba que dispone de un tipo de acceso que permite la autenticación externa, se permite el acceso del usuario al producto.
2. Cuando no se ha producido ninguna autenticación externa, CA Service Desk Manager solicita al usuario que indique su ID de usuario y contraseña. El producto busca un registro de contacto para el ID de usuario, obtiene el tipo de acceso y, por último, autentica al usuario según lo especifique dicho tipo.

En muchas instalaciones, los tipos de acceso predefinidos definen un tipo de autenticación adecuado para el tipo de usuario al que se aplican. No obstante, en algunos casos, es necesario modificar los datos de autenticación pertenecientes a algún tipo de acceso predefinido, o bien, definir nuevos tipos de acceso para gestionar métodos de autenticación distintos para algunos de los usuarios. Conviene revisar los valores de la autenticación en los tipos de acceso predefinidos con el fin de averiguar si satisfacen las necesidades, si hace falta modificarlos o si es preciso definir otros tipos.

Autenticación externa

CA Service Desk Manager permite que los usuarios accedan al sistema sin suministrar ningún ID de usuario, siempre que se cumplan todas las condiciones siguientes:

- Se estableció la autenticación externa para el usuario.
- La ID de usuario que se autenticó de forma externa se asocia a un contacto de la tabla de contactos.
- El registro de contacto tiene un tipo de acceso cuya definición de autenticación permite la autenticación externa.

La autenticación externa no permite que los usuarios accedan al sistema en los siguientes casos:

- Un usuario intenta acceder a través de un servidor no seguro.
- Un usuario intenta acceder, pero se asigna a un tipo de acceso que no permite la autenticación externa.

Ninguno de los tipos de acceso predefinidos utiliza la autenticación externa. Si quiere utilizar la autenticación externa para usuarios, considere modificar el tipo de acceso de empleado, analista y administrador. Los requisitos de cada sitio y los distintos tipos de usuarios son los factores que determinan la aceptación de la autenticación externa. Cuando se utiliza ésta, la configuración del servidor controla el acceso a los archivos y a los directorios. Cuando define la autenticación para un tipo de acceso, puede decidir el uso de la siguiente forma:

- No utilice la autenticación externa que ya se implementa, como el inicio de sesión de usuario en Windows o la validación por el servidor HTTPD.
- Utilice la autenticación que se implementa y permita o niegue que el acceso según ella.

Nota: Si no se permite la autenticación externa, el usuario se autentica según el tipo de validación que se especifique.

A continuación, se describen algunos ejemplos de autenticación externa:

- Si un usuario que tiene acceso de administrador inicia sesión en un equipo con Windows, el usuario puede ejecutar tareas administrativas sin tener que volver a introducir la información de inicio de sesión.
- Si un usuario tiene validación de servidor HTTPD, el usuario puede acceder a la interfaz Web sin tener que volver a introducir la información de inicio de sesión. Dado que el tipo de acceso de administrador especifica el tipo de usuario Web de analista, se presenta de manera automática la interfaz Web para los analistas.

Tipos de validación

Los tipos de validación autentican a los usuarios sólo en las siguientes circunstancias:

- El tipo de acceso del usuario no permite la autenticación externa.
- El tipo de acceso del usuario permite la autenticación externa pero no se ha validado al usuario externamente (por ejemplo, si el usuario ha tratado de acceder a través de un servidor no seguro).

CA Service Desk Manager le ofrece las siguientes opciones de validación:

- **Ningún acceso:** los usuarios de este tipo no tienen acceso a menos que la autenticación externa esté permitida y sea válida.
- **Abrir:** los usuarios de este tipo disponen de acceso sin que se exija ninguna otra autenticación.
 - **SO:** los usuarios de este tipo introducen su contraseña del sistema operativo para acceder. El sistema operativo utilizado para la validación es en el que se ejecuta el host de validación de usuarios. Esta opción es el tipo de validación predeterminado para los tipos de acceso de administrador, analista y empleado.
 - **PIN:** los usuarios de este tipo obtienen acceso indicando como contraseña el valor del campo PIN de su registro de contacto. El campo PIN se define mediante la especificación del nombre de atributo del campo al seleccionar PIN como tipo de validación. Este tipo de validación es el predeterminado para el tipo de acceso de cliente, que emplea el valor del campo ID de cliente (contact_num) como PIN.

Nota: Para obtener una lista de los nombres de atributo para el objeto cnt, que es el objeto definido para la tabla Contacto, consulte la *Guía de referencia técnica*.

Recuentos de usuarios con licencia y conectados

El KPI webLicenseCt cuenta el número de usuarios conectados que están utilizando una licencia de CA Service Desk Manager. La casilla de verificación Con licencia? en la página Tipo de acceso determina si este contacto es un tipo de acceso con licencia. Los contactos asignados a tipos de acceso sin licencia sólo pueden ver o actualizar sus propios datos personales. Además, el KPI webSessionCt cuenta el número total de sesiones Web: se cuentan tanto los usuarios analistas con licencia como los usuarios finales que inician sesión en la interfaz Web de autoservicio. Si un usuario inicia sesión varias veces en CA Service Desk Manager, ya sea en su equipo o en otro equipo, se producen varias sesiones Web. Si el usuario es un analista, se utilizan varias licencias. Varias páginas abiertas para el usuario conectado no afectan a la sesión Web y al recuento de licencias Web.

Nota: Para obtener más información sobre tipos de acceso, consulte la *Ayuda en línea*.

Ejemplo: recuentos de usuarios con licencia y conectados

Tres usuarios finales están conectados a la interfaz Web de autoservicio y revisan algunos anuncios.

Al mismo tiempo cinco analistas con licencia (que tienen el ticket de casilla de verificación en su tipo de acceso) están conectados a la interfaz de analista y trabajan en incidentes.

El KPI webLicenseCt muestra un recuento de cinco, lo que significa que se están usando cinco licencias en este momento.

El KPI webSessionCt muestra un recuento de ocho, lo que significa que ocho usuarios en total están conectados a la interfaz Web de CA Service Desk Manager.

Registros internos

Cabe la posibilidad de definir si los tipos de acceso pueden o no consultar los registros internos. En caso afirmativo, los contactos ven una casilla de verificación con la etiqueta Interno en todas las ventanas Actividades de registro, que se puede seleccionar para que la actividad en cuestión se considere interna. Si las actividades están marcadas como internas, sólo pueden verlas y recibir notificaciones sobre ellas los contactos con un tipo de acceso que permita consultar los registros internos.

Integración de CA Service Desk Manager

El tipo de acceso identifica, asimismo, el tipo de usuario que se pone en contacto con él cuando utilizan otros productos de CA con CA Service Desk Manager. Cuando un contacto con ese tipo de acceso utiliza el otro producto, sus derechos de usuario sobre ese producto se ven determinados por los valores especificados en el tipo de acceso.

Asociaciones de partición de datos

Se pueden asignar particiones de datos a contactos individuales, pero el método preferido es asignar particiones de datos basadas en el tipo de acceso. Una vez asociadas las particiones de datos con distintos tipos de acceso, puede asociar un contacto a un tipo de acceso particular y, así, definir su partición de datos. El tipo de acceso tiene una opción específica para sustituir la partición de datos de contacto.

Para asociar una partición de datos a un tipo de acceso, puede establecer particiones de datos que sean significativas para su sitio y luego seleccionar una de las particiones de datos cuando defina o modifique un tipo de acceso.

Importante: Otros valores de seguridad de CA Service Desk Manager pueden tener prioridad sobre la partición de datos.

Particiones de datos

Las particiones de datos son subconjuntos de las bases de datos de CA Service Desk Manager que controlan el acceso de los usuarios a los tickets y a otros registros de datos en función del contenido. Por ejemplo, puede restringir la visualización de una base de datos por parte de un usuario sólo a aquellos elementos de configuración que estén asignados a la organización del usuario. También es posible limitar el acceso de un usuario para que únicamente pueda actualizar los tickets asignados y permitir un acceso de-sólo lectura a los demás elementos de configuración.

Las particiones de datos constan de un conjunto de restricciones. Estas restricciones identifican las tablas que controlan las particiones de datos así como el tipo de restricción. Los tipos de restricciones especifican qué puede hacer el usuario en la partición de datos, es decir, crear, eliminar, actualizar, ver, etc. Tras asignar una partición de datos a un tipo de acceso que posteriormente asigna al registro de contacto de un usuario, las restricciones y los tipos de restricciones son los que controlan el acceso del usuario a los registros de la tabla de base de datos de CA Service Desk Manager.

Asimismo, existe la opción de ver las restricciones con independencia de la partición de datos que las use. Resulta útil porque, en ocasiones, conviene consultar todas las restricciones que se aplican a una tabla determinada sin que importe la partición.

Nota: Si desea obtener más información sobre cómo usar las restricciones de partición de datos, consulte la *ayuda en línea*.

Configuración de particiones de datos

Se puede definir un número ilimitado de particiones de datos. Cada partición de datos consta de un conjunto de restricciones y validaciones aplicables a las tablas de bases de datos que restringe la partición. Para cada una de las tablas de las particiones de datos, se pueden indicar autorizaciones independientes para ver, actualizar, crear o eliminar registros empleando criterios que se especifican con un formato parecido a las cláusulas WHERE de SQL. Las restricciones se pueden basar en cualquier atributo de los registros a los que se pretende acceder combinado con cualquier dato de los registros de contactos de los usuarios. Este método favorece la flexibilidad a la hora de definir las particiones de datos. Por ejemplo, al utilizar el campo Distribuidor de la tabla Contacto, se facilita la imposición de las restricciones de la partición de datos oportuna a los distribuidores con permiso para acceder directamente a CA Service Desk Manager.

por motivos de rendimiento, CA Service Desk Manager no permite que las restricciones de las particiones de datos contengan uniones cartesianas. Éstas se producen cuando las restricciones incluyen un nexos "O" que restringe por completo todas las tablas unidas a ambos lados del nexos. Para asegurarse de que las restricciones de las particiones de datos no produzcan ninguna unión de producto cartesiano, escriba el siguiente comando:

Windows

```
bop_cmd -f $NX_ROOT\bopcfg\interp\bop_diag.frg "check_queries()"
```

UNIX

```
bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"
```

Importante: Todas las particiones de datos marcadas por este programa se deben actualizar en consecuencia. Para obtener más información sobre cómo definir particiones de datos, restricciones y tipos de límites, consulte la *ayuda en línea*.

Especificaciones de las restricciones

Las restricciones y las pruebas de validación se especifican en Majic con el metalenguaje de definición de objetos.

Nota: Para obtener información, consulte la *Guía de referencia técnica*.

Las restricciones definidas en Majic presentan una enorme semejanza con las cláusulas WHERE de SQL salvo por las siguientes excepciones:

- Los nombres de los atributos de la restricción son nombres de atributos de objetos, no el nombre del atributo de base de datos del esquema.
- Es posible hacer referencia al valor de los atributos del registro de contacto del-usuario que inició sesión mediante un nombre con el formato siguiente, donde *att_name* es el nombre en Majic del atributo deseado:

`@root.att_name`

Por ejemplo, `@root.location` hace referencia al ID de la ubicación del contacto actual.

Las uniones se especifican con el formato siguiente, donde *foreign-key* es el nombre en Majic del atributo SREL de la tabla para el que se elabora la restricción de la partición de datos y *attribute-in-referenced-table* es el nombre en Majic del atributo de la tabla que se une:

`foreign-key.attribute-in-referenced-table`

Por ejemplo, para hacer referencia al distribuidor de mantenimiento del activo asociado a un informe de incidente, especifique lo siguiente:

`resource.vendor_repair`

Esta especificación se repite. Por ejemplo, se puede hacer referencia al nombre del distribuidor con lo siguiente:

`resource.vendor_repair.name`

En la siguiente tabla se presentan ejemplos de restricciones válidas que se utilizarán para la tabla `Change_Request`, empleada para almacenar la información de las órdenes de cambios:

Tipo de restricción	Código y descripción
Vista	<code>assignee.organization = @root.organization</code> Especifica que el usuario sólo puede ver las órdenes de cambios si la organización del asignatario es la misma que la del usuario.
Pre-Update	<code>requestor = @root.id</code> Especifica que el usuario sólo puede actualizar las órdenes de cambios si es el autor de la llamada o el solicitante.

Sin embargo, no es posible escribir una restricción que use uniones en ambos lados de la expresión como la del ejemplo siguiente:

```
assignee.org = requestor.org
```

Tipos de restricciones

Se pueden asignar los siguientes tipos de restricción en cada una de las tablas controladas en las particiones de datos:

Crear

Especifica criterios que se deben cumplir para crear registros. Si un usuario de una partición de datos trata de crear un registro que no coincide con la condición de prueba de creación, CA Service Desk Manager muestra el mensaje de error asociado a la restricción y no guarda el registro.

Valores predeterminados

Especifica una instrucción de asignación (o varias separadas por punto y coma) que define los valores que se deben asignar a los campos vacíos de los registros nuevos en el momento de almacenar éstos. La sintaxis de las instrucciones de asignación es la siguiente, donde *att_name* es el nombre de un atributo Majic del registro y *value* puede ser un número entero, una cadena entre comillas o una referencia con el formato *@root.att_name* a un atributo Majic del registro de contacto del usuario actual:

```
att_name=value
```

En el caso de las tablas actualizadas para los partes, los valores predeterminados se colocan en el registro en el momento en el que se muestra y aparecen al presentar por primera vez el nuevo registro. Si se desean asignar valores predeterminados a campos de referencia (SREL de Majic), es necesario codificarlos con el formato de los ID persistentes. Los ID persistentes son nombres de objetos seguidos de dos puntos y un ID de número entero. Por ejemplo, es posible definir un valor predeterminado para una categoría incluyendo lo siguiente en la especificación de valores predeterminados, donde PCAT es el destino de SREL (como figura en el archivo Majic) y 12345 es el número de ID de la categoría deseada:

```
category='PCAT:12345'
```

Para ver los ID persistentes de los objetos, sírvase de un comando con este formato:

```
bop_odump domsrvr pcat "" sym
```

Suprimir

Especifica criterios que se deben cumplir para eliminar registros. Si un usuario de una partición de datos trata de suprimir un registro que no coincide con la condición de prueba de supresión, CA Service Desk Manager muestra el mensaje de error asociado a la restricción y no suprime el registro.

Pre-Update

Especifica los registros de las tablas controladas que el usuario puede actualizar en las particiones de datos. Si un usuario de la partición de datos solicita un registro que no coincide con la condición de preactualización, CA Service Desk Manager lo convierte en un registro de sólo lectura y muestra el mensaje de error definido con la restricción.

Actualizar

Especifica criterios que se deben cumplir para guardar registros. Si un usuario de una partición de datos trata de guardar un registro que no coincide con la condición de actualización, CA Service Desk Manager muestra el mensaje de error asociado a la restricción y no guarda el registro.

Vista

Especifica los registros de las tablas controladas que el usuario puede consultar en las particiones de datos. Esta restricción se aplica automáticamente a todas las listas que seleccione un usuario en esta partición de datos, además de a cualquier criterio de selección que el usuario especifique de forma explícita.

Esta restricción puede incluir uniones a otras tablas y referencias con el formato `@root.att_name` a atributos Majic del registro de contacto del usuario actual o conectado. Éstos son algunos ejemplos válidos:

```
requestor.organization = @root.organization  
requestor.organization.name = 'MIS'  
assignee = @root.id  
assignee.organization = @root.organization
```

Nota: Ahora puede crear, suprimir, pre actualizar y actualizar tipos de restricciones con uniones de otras tablas. Pueden incluir también referencias en el formulario `@root.attribute` a atributos en el registro de contacto para el usuario actual.

Creación de restricciones de partición de datos para asignaciones de CAB

Se puede crear una restricción de partición de datos que permita a los usuarios actualizar sólo órdenes de cambio asignadas a un CAB al que pertenezca el usuario conectado.

Para crear una restricción de partición de datos para asignaciones de usuarios de órdenes de cambio de CAB, asigne los valores de restricción siguientes relativos a una tabla controlada Change_Request en una partición de datos:

- Tipo de restricción: Preactualización
- Especificación de restricción: cab.[group]group_list.member IN (@root.id)

El usuario conectado sólo puede actualizar órdenes de cambio que estén asignadas a un CAB al que pertenezca dicho usuario.

Más información:

[Generación de informes y Consola de CAB](#) (en la página 693)

Configuración de restricciones para la partición de datos de Gestión del conocimiento para permisos basados en roles

Las particiones de datos de Gestión del conocimiento están habilitadas para permitir el uso de permisos de rol y grupo de forma predeterminada en CA Service Desk Manager. Si va a actualizar de una versión anterior, la herramienta de migración actualiza las restricciones para la partición de datos.

Si utilizó restricciones para la partición de datos personalizadas para gestionar permisos de conocimiento en una versión anterior, actualice las restricciones manualmente para las tablas O_INDEXES y SKELETONS. Puede ver las restricciones para la partición de datos predeterminadas y aplicar los cambios, según sea necesario para su entorno.

Procedimiento para actualizar las restricciones para la partición de datos

1. En la ficha Administración, vaya a Gestión de seguridad y de roles, Particiones de datos, Restricciones para la partición de datos.
Aparecerá la lista de restricciones de partición de datos.
2. Haga clic en Mostrar filtro.
Aparecerá el filtro de búsqueda.
3. Escriba **Analista de Service Desk** en la búsqueda de particiones de datos
4. Escriba **O_INDEXES** en la búsqueda de tabla.
5. Haga clic en Buscar.
Aparecerán los resultados de la búsqueda.
6. Haga clic en el tipo *Ver restricción*.
Aparecerá la página Detalles de restricción de partición de datos.
7. Haga clic en Editar.
Aparecerá la página Actualizar restricción de partición de datos.
8. Modifique la ficha Restricción para reemplazar "READ_PGROUP in @root.pgroups" de la siguiente forma:

```
READ_PGROUP in @root.pgroups OR  
READ_PGROUP.[pgroup]contained_roles.role IN @root.id
```


Guarde la restricción.
9. Abra los tipos de restricción *Suprimir* y *Actualización previa* en la Lista de restricciones para la partición de datos.
10. Modifique la ficha Restricción para reemplazar "WRITE_PGROUP in @root.pgroups" en *Suprimir* y *Actualización previa* de la siguiente forma:

```
WRITE_PGROUP in @root.pgroups OR WRITE_PGROUP.[pgroup]contained_roles.role IN @root.role
```

11. Guarde las restricciones.
12. Repita los pasos para actualizar las restricciones *Ver, Suprimir y Actualización previa* en la tabla *SKELETONS* de la partición de datos.

Las restricciones para la partición de datos se actualizan.

Encuestas

Las encuestas de clientes permiten a los administradores de CA Service Desk Manager recopilar y analizar de forma sistemática la opinión de los clientes en cuando al funcionamiento del servicio de asistencia. Puede personalizar las encuestas para adaptarlas a las necesidades de su sitio.

Configuración del sistema para incluir estudios

Para poder usar los estudios, es preciso configurar el sistema de manera adecuada, proceso que consta de dos pasos:

1. Instalar y configurar la interfaz Web de CA Service Desk Manager. Cada vez que los usuarios acceden a la dirección URL de un estudio, la interfaz Web le da el formato apropiado y se introducen los datos pertinentes. Para obtener más información, consulte la *Guía de implementación*.
2. Configurar e instalar con el gestor de opciones la opción `web_cgi_url` a fin de especificar la ubicación del motor Web de CA Service Desk Manager. Si desea obtener detalles, consulte el capítulo "Control del comportamiento del sistema" y la *ayuda en línea*.

Preparación de estudios

Los estudios se preparan con la ayuda de la ventana de lista típica Lista de estudios de clientes. En esta ventana se ven todos los estudios o un conjunto de ellos de acuerdo con los criterios de búsqueda indicados, se crean estudios nuevos, se consultan los detalles de los estudios y se generan informes sobre los estudios que aparecen en la lista, entre otras acciones.

Todos los estudios poseen las características siguientes, que son susceptibles de definición:

- Nombre, que resulta de utilidad con fines de búsqueda y creación de informes.
- Introducción, que se utiliza para explicar el objetivo del estudio a los clientes.

- Lista ordenada de preguntas que debe responder el cliente, cada una de las cuales incluye un conjunto de posibles respuestas.
- Área opcional donde el usuario escribe sus observaciones si lo desea.
- Mensaje de estudio completado, que se muestra una vez enviado el estudio.

Nota: Si desea obtener más información sobre la creación de encuestas, consulte la *ayuda en línea*.

Definición de notificaciones de encuesta

La ficha Encuesta en la página Actualizar notificaciones de actividades permite definir una notificación de encuesta para una notificación de actividades. Cuando se activa la notificación de actividades seleccionada, el contacto que haya iniciado la actividad recibe la notificación de encuesta. Se genera un registro de actividades tanto al enviar la notificación de estudio como al recibir el estudio del cliente.

Procedimiento para configurar una notificación de encuesta

1. En la ficha Administración, vaya a Notificaciones, Notificaciones de actividades.
Aparecerá la lista de notificaciones de actividades.
2. Seleccione la notificación de actividad deseada.
Aparecerá la página de detalles.
3. Haga clic en el botón Editar.
Aparecerá la página Actualizar notificaciones de actividades.
4. Edite los campos según sea necesario.
5. Seleccione el tipo de objeto adecuado en la lista desplegable.
6. Haga clic en la ficha Encuesta.

Esta ficha contiene los siguientes campos:

Enviar estudio

Esta casilla de verificación permite activar o desactivar la encuesta. Si está seleccionada, la encuesta se envía al contacto cuando se activa la notificación de actividades seleccionada.

Estudio predeterminado

Especifique una encuesta predeterminada mediante el icono de búsqueda o especifique su propia encuesta en el cuadro de texto.

Método de notificación

Seleccione *uno* de los siguientes métodos de notificación:

- Correo electrónico
- Notificación
- Pager_Email

Título del mensaje de estudio

Escriba el título de la encuesta.

Cuerpo del mensaje de estudio

Escriba un mensaje para el contacto. Cuando un contacto recibe la notificación de alguna encuesta, se incluye automáticamente una dirección URL en el cuerpo del mensaje en la que se puede hacer clic para acceder al formulario de la encuesta en el explorador Web y poder rellenarlo.

7. Guarde la notificación de actividades.

Cuando se activa la notificación de actividades seleccionada, el contacto que haya iniciado la actividad recibe la notificación de encuesta.

Generación de informes sobre estudios

CA Service Desk Manager facilita la generación de informes sobre los estudios en la ficha de administración de los clientes Web tal como se suelen crear. Para ello, por ejemplo, en la ventana Lista de estudios de clientes, elija la opción Informes en el menú Archivo y, a continuación, la opción Informe resumido o la opción Informe detallado. Además, si se quieren imprimir los datos de los estudios, las preguntas y las respuestas, se puede elegir la opción Imprimir formulario en las diversas ventanas de detalles.

Otra posibilidad consiste en diseñar informes propios basándose en los datos de los estudios que se mantienen en la base de datos de CA Service Desk Manager.

Encuesta gestionada

La función de estudios gestionados permite al administrador de CA Service Desk Manager seleccionar un conjunto de ejemplo del estudio deseado y cotejarlo con un estudio específico. A continuación, el administrador puede distribuir las solicitudes de destino para que los encuestados realicen el estudio en un momento específico. De este modo, el administrador disfruta de la flexibilidad de abrir períodos de encuesta al tiempo que mantiene la capacidad para elaborar encuestas basadas en las actividades y las categorías que estén relacionados con las solicitudes, las órdenes de cambio y las incidencias.

El objetivo de esta función consiste en proporcionar un mecanismo para gestionar las encuestas. Resulta de gran utilidad en el caso de los formularios de encuesta que se deben supervisar cada cierto tiempo, por ejemplo, las encuestas que se utilizan todos los años durante un plazo breve o las encuestas que llevan demasiado tiempo sin usar.

Nota: Para obtener más información, consulte la *ayuda en línea*.

Servicios Web

Los servicios Web se ajustan a estándares de intercambio de datos que realizan lo siguiente:

- Permitir que las aplicaciones se comuniquen por HTTP con diferentes servidores de cualquier entorno operativo.
- Permitir que la mayoría de las aplicaciones puedan acceder a la funcionalidad del producto de CA.
- Permitir que los clientes de servicios Web puedan crear tickets, actualizar activos, buscar en la base de conocimiento y mucho más.

Nota: Para obtener más información, consulte Gestión de servicios Web en la *Guía de implementación*.

Capítulo 5: Configuración de cuentas de usuario

Esta sección contiene los siguientes temas:

[Contactos](#) (en la página 199)

[Definiciones de contactos](#) (en la página 200)

[Grupos](#) (en la página 201)

[Tipos de contactos](#) (en la página 202)

[Tipos de tratamientos especiales](#) (en la página 203)

[Datos del directorio LDAP](#) (en la página 206)

Contactos

Una parte importante del establecimiento y la puesta en funcionamiento de un servicio de asistencia consiste en definir los usuarios que van a acceder a él. En CA Service Desk Manager, los usuarios son denominan *contactos* y puede ejecutar varias tareas para configurarlos y gestionarlos:

- Configurar los contactos manualmente.
- Organizar los contactos en grupos que definan áreas de responsabilidad.
- Establecer tipos de contactos para organizar los contactos de CA Service Desk Manager en agrupaciones lógicas según el uso que hagan del sistema.
- Importar información de usuario de LDAP a un registro de contacto de CA Service Desk Manager.
- Asignar un contacto a un rol para definir la funcionalidad del sistema accesible.
- Asignar un tipo de tratamiento especial, como Persona muy importante (VIP), a un contacto.

Definiciones de contactos

Toda persona que use CA Service Desk Manager debe estar definida como contacto. El registro de contacto de un usuario define la información de usuario que el sistema necesita, de la siguiente manera:

Identificación básica

Define una identificación básica, como el nombre de usuario y el tipo de contacto. El nombre de los contactos sirve como identificador principal al seleccionarlos o rellenar los datos de un contacto en otros contextos.

Inicio de sesión

Define la información de inicio de sesión, como ID de usuario y, en algunos casos, un campo PIN para utilizar como una contraseña que verifica el usuario en el inicio de sesión. Ese ID se usa para identificar al usuario en la tabla de contactos con fines de autenticación y para determinar los tipos de acceso asignados al usuario. Según la configuración de seguridad por la que haya optado el administrador, se puede especificar otro campo; por ejemplo, ID de contacto, como campo PIN, que sirve al usuario como contraseña para el inicio de sesión.

Seguridad

Define el tipo de acceso que se asigna en su registro de contacto o por un tipo de acceso predeterminado, según cómo configuró la seguridad para el sistema. El tipo de acceso de un usuario también se puede asignar según la pertenencia a grupos de los directorios LDAP.

El tipo de acceso de los usuarios determina todos los aspectos de su seguridad, incluidos el modo en el que se autentican en el sistema, la interfaz Web que ven o las funciones del producto a las que tienen acceso.

La gestión de la seguridad es una función de la interfaz Web.

Tipo de servicio

Determina el nivel de servicio que recibe un usuario. El tipo de servicio de los contactos define el nivel que deben recibir los usuarios. Los acuerdos de nivel de servicio se negocian con los clientes de CA Service Desk Manager y los tipos de servicios actúan como mecanismo de CA Service Desk Manager para implementarlos. Mediante la asociación de los tipos de servicios a los registros de contactos de los usuarios, es posible garantizar que, cuando se cree un ticket con el cual se identifica un usuario como el usuario final afectado, el tipo de servicio del ticket será, como mínimo, igual que el del contacto.

La configuración de los acuerdos de nivel de servicio mediante el uso de tipos de servicios es una función que usted, como administrador, realiza con la interfaz Web.

Asignación automática

Define la información de asignación automática, como los turnos de trabajo y la disponibilidad (utilizados sólo para tipos de contactos que sean analistas). Es posible configurar contactos de analistas para determinar si son aptos para la asignación automática. La asignación automática sólo es válida para las solicitudes y se establece como parte de la definición de las áreas de solicitud. Además, está vinculada a los grupos a los que pertenece el analista.

Información acerca de cómo enviar mensajes de notificación a los usuarios

Define la información de notificación de los contactos que incluye diversas direcciones de correo electrónico y números de teléfono que pueden usarse con fines de notificación, el método preferido para las notificaciones según su urgencia y los turnos durante los cuales se deben recibir.

La información de las organizaciones (como la ubicación, la organización y el departamento) permite agrupar los contactos según la organización a la que pertenecen. Por ejemplo, si se asocia un contacto a una ubicación, se vincula dicho contacto a una dirección física, lo que facilita la asignación automática. También se pueden asignar los tipos de servicios a las organizaciones y facilitar, de este modo, la gestión de acuerdos de nivel de servicio ya que se realiza por organización en lugar de por contacto.

Grupos a los que pertenecen los usuarios

Los contactos se pueden organizar por grupos que representen áreas específicas de responsabilidad dentro de su centro de servicio al usuario. Los contactos se pueden configurar y definir en la interfaz Web.

Grupos

Los grupos son recopilaciones de contactos que comparten un área de responsabilidad común. En CA Service Desk Manager, los grupos se implementan mediante el tipo de contacto predefinido de grupo, lo que convierte a los grupos en un mero tipo especial de contacto. Los grupos disponen de la misma información básica que los contactos, con la importante función adicional de que los primeros resultan fundamentales para la asignación automática de las solicitudes. A los grupos se pueden asociar áreas de solicitud, ubicaciones o turnos. Estos atributos se emplean para determinar si los contactos del grupo están disponibles para la asignación automática de solicitudes y cuándo.

Nota: Para obtener información acerca de cómo definir grupos, consulte la *ayuda en línea*.

Tipos de contactos

Los tipos de contactos se emplean para categorizar los usuarios de CA Service Desk Manager en agrupaciones lógicas según cómo usen el sistema. El sistema, por ejemplo, cuenta con numerosos tipos de contactos predefinidos, como analista, de cliente o grupo. Estos tipos de contacto predefinidos satisfacen las necesidades de la mayor parte de las implementaciones de CA Service Desk Manager; sin embargo, si sus circunstancias lo requieren, puede modificar los tipos de contacto predefinidos y crear tipos de contacto. Cuando defina los usuarios como contactos, puede asociar un tipo de contacto a cada uno.

Nota: Para obtener más información acerca de cómo definir tipos de contactos, consulte la *ayuda en línea*.

Determinación del comportamiento según los tipos de contactos

El *tipo* de contacto condiciona qué contactos se muestran (y disponen de permiso) en distintas situaciones. Así, por ejemplo, si se asigna de forma manual cualquier tipo de parte, como una solicitud o una incidencia, el campo donde se especifica el asignatario requiere que se indique una persona cuyo tipo de contacto sea de analista. La lista de selección disponible en el campo sólo muestra los contactos con el tipo de analista. Si se indica otro contacto cuyo tipo sea diferente, aparece sólo la pantalla de búsqueda de analistas.

Nota: Una función importante de los tipos de contactos consiste en la implementación de grupos de contactos mediante el tipo de grupo predefinido.

Configuración de notificaciones según el tipo de contacto

La notificación se puede basar en los tipos de contactos; así, es posible enviar mensajes de notificación a todos los contactos de un tipo en particular.

Más información:

[Notificaciones](#) (en la página 93)

Selección de contactos según los tipos de contactos

Es posible seleccionar los usuarios según su tipo de contacto en diversos contextos. Por ejemplo, casi todas las ventanas de lista y selección donde se muestran contactos disponen de campos de búsqueda en los que se puede especificar el tipo de contacto como criterio.

Tipos de tratamientos especiales

Puede definir tipos de tratamiento especial que identifican contactos que requieren atención diferencial. Puede utilizar los tipos de tratamiento especial que CA Service Desk Manager proporciona o crear sus propios tipos. Puede ver y localizar tickets que especifican un usuario final afectado que requiere atención especial. Por ejemplo, los analistas pueden examinar la carpeta V.I.P. en el panel de resultados para identificar los tickets que especifican un VIP como el usuario final afectado.

Los ejemplos siguientes constituyen contactos que los tipos de tratamiento especial pueden identificar:

- Personas muy importantes (VIP), como ejecutivos
- Clientes que tienen la renovación del soporte en proceso
- Clientes con discapacidades que requieren equipamiento o tratamiento especial
- Visitantes
- Contactos sospechosos de hacer mal uso o abusar de los recursos del sistema

Cuando se asigna uno o más tipos de tratamiento especial a un contacto, los tickets que especifican el contacto en el campo Usuario final afectado muestran un icono o banner de alerta, o ambos al mismo tiempo. Puede utilizar campos de ticket y tipos de tratamientos especiales para hacer un seguimiento de los tickets, así como para distinguir entre dos tipos de contactos relacionados pero posiblemente distintos. Por ejemplo, un VIP (Usuario final afectado) tiene un ayudante (Solicitante) que actúa en su nombre. Cuando el usuario final afectado es un contacto asignado a un tipo de tratamiento especial VIP, un analista puede dar prioridad a los tickets con más precisión.

Más información:

[Cómo configurar contactos de tratamiento especial](#) (en la página 204)

[Cómo asociar un contacto a un tipo de tratamiento especial](#) (en la página 205)

Más información

[Cómo asociar un contacto a un tipo de tratamiento especial](#) (en la página 205)

Cómo configurar contactos de tratamiento especial

Para configurar contactos de tratamiento especial, realice los siguientes pasos:

1. Cree los tipos de tratamientos especiales.
2. Asocie un contacto a cualquier número de tipos de tratamiento especial (see page 205). Del mismo modo, un tipo de tratamiento especial puede tener muchos contactos.

Mediante el uso de un banner ubicado en la parte superior de cada página, se distingue visualmente un contacto asociado con uno o más tipos de tratamiento especial en el formulario Detalles de contacto y en el explorador de Perfil rápido. Este banner muestra el icono de alerta y el texto de alerta para cada tipo de tratamiento especial asignado al contacto.

Adicionalmente, algunos tickets que identifican al contacto como el usuario final afectado se indican de la siguiente manera:

- Aparecen iconos de alerta y texto de alerta en el banner ubicado en la parte superior del formulario de detalles del ticket.
- Aparecen iconos de alerta en la lista de tickets.
- El panel de resultados incluye una carpeta V.I.P. y subcarpetas para cada tipo de ticket. Las subcarpetas de V.I.P. incluyen tickets para los usuarios finales afectados que son contactos de tratamiento especial VIP.

Nota: Se muestra la carpeta V.I.P. del panel de resultados para los roles de analista.

Cómo asociar un contacto a un tipo de tratamiento especial

Puede asignar un tipo de tratamiento especial a un contacto para alertar a los analistas sobre tickets que afectan a usuarios finales con requisitos especiales, como a una persona con discapacidades visuales, un contacto que plantea un riesgo de seguridad, etc.

Cómo asociar un contacto a un tipo de tratamiento especial

1. En la página Detalles de contacto, seleccione la ficha Tratamiento especial.
La ficha Lista de tratamientos especiales asociados lista los tipos de tratamiento especiales que se asocian con el contacto.
2. Haga clic en el botón Actualizar tratamientos especiales de contacto.
Aparecerá el filtro de búsqueda.
3. Busque el tipo de tratamiento especial que quiere asociar al contacto.
Aparecerá la página Actualizar tratamiento especial.
4. Seleccione uno o más tipos de tratamiento en la columna de la izquierda y utilice el botón de movimiento (>>) para mover los tipos a la columna derecha. Haga clic en OK.

Nota: Puede eliminar una asociación de un contacto utilizando el botón de movimiento (<<) para mover el tipo de la columna derecha a la columna izquierda. Puede hacer clic en el icono de búsqueda para buscar el valor que desee.

El contacto se asocia a un tipo de tratamiento.

CA Service Desk Manager muestra alguna de las siguientes opciones, dependiendo del tipo de tratamiento, cuando un ticket especifica el contacto en el campo Usuario final afectado:

- Aparecerá un banner de alerta en Detalles de contacto para el usuario final afectado en un ticket.
- El texto de alerta aparecerá con el formato de un banner en la parte superior de la página de detalles del ticket y en Perfil rápido.
- Las listas de ticket resaltan la fila de contacto y muestran un indicador de alerta.
- Aparecerá una carpeta V.I.P. en el panel de resultados para los roles de analista. La carpeta contiene todos los tickets que están asociados con contactos (Usuarios finales afectados) que tienen un tipo de tratamiento especial VIP.

Datos del directorio LDAP

El *Protocolo ligero de acceso a directorios* (LDAP) es un protocolo de comunicaciones de red para consultar y modificar servicios de directorio que se ejecutan en una red TCP/IP. Un directorio LDAP es una estructura de árbol que contiene entradas para gestionar usuarios, grupos, equipos, impresoras y otras entidades de una red.

Se puede configurar CA Service Desk Manager para acceder a un directorio LDAP, que le permite utilizar datos LDAP de varias maneras:

- Sincronizar contactos con registros de los usuarios de LDAP. La sincronización puede llevarse a cabo de las siguientes maneras:
 - **En el inicio de sesión:** cuando un usuario se conecta al producto, si un registro LDAP existe para ese usuario, pero no existe un registro de contacto correspondiente, se crea un registro de contacto automáticamente según la información de LDAP.
 - **Nuevo contacto:** cuando crea un registro de contacto en forma manual, puede seleccionar un registro LDAP y combinar sus valores de atributo con sus campos correspondientes en el nuevo registro de contacto.
 - **Actualización por lotes:** puede ejecutar trabajos por lotes para automatizar los procesos de importación y actualización de registros de contacto con información de los registros LDAP correspondientes.
- Nota:** La sincronización con LDAP es un proceso unidireccional. Los datos LDAP se pueden utilizar para crear y actualizar contactos, pero el producto no admite actualizaciones al directorio LDAP.
- Asigne tipos de acceso de CA Service Desk Manager según la pertenencia a los grupos de LDAP.
 - Implemente un método alternativo de autenticación de CA Service Desk Manager.

Nota: El componente ldap_virtb proporciona la funcionalidad de integración de LDAP, se instala con CA Service Desk Manager en forma predeterminada y puede ejecutarse en un servidor primario o secundario, independientemente del tipo de sistema operativo. Para obtener información, consulte la *Guía de implementación*. El archivo \$NX_ROOT/bopcfg/majic/ldap.maj especifica la asignación entre atributos LDAP y atributos de registro de contacto.

Importante: CA Service Desk Manager exige que los registros LDAP tengan una entrada en el campo Apellido para buscar, ver e importar los datos de LDAP.

Importante: CA Service Desk Manager admite la *búsqueda paginada*, mediante la cual se realizan búsquedas de todos los registros del directorio LDAP. La búsqueda paginada también le permite importar nuevos registros de contacto o sincronizar registros de contactos existentes de cualquier cantidad de registros LDAP. Sin embargo, estas capacidades están limitadas si está utilizando el servidor de directorio SunOne o Novell eDirectory, dado que estos servidores LDAP no admiten la búsqueda paginada. En ese caso, solo puede buscar, importar y sincronizar la cantidad de registros de LDAP especificados por NX_LDAP_MAX_FETCH. Para obtener más información, consulte la sección Archivo NX.env (see page 223).

Configuración de las opciones de LDAP

Puede configurar CA Service Desk Manager para acceder a los datos del directorio LDAP.

Procedimiento para configurar CA Service Desk Manager y tener acceso a los datos del directorio LDAP

1. Instale manualmente las opciones de LDAP con el Gestor de opciones de la interfaz Web.

Nota: Las opciones necesarias para la integración básica de LDAP están identificadas como obligatorias en la columna Descripción en la tabla siguiente. Las opciones identificadas como opcionales son funciones que sólo se pueden agregar si las opciones obligatorias están instaladas. Los valores que se especifican al instalar estas opciones se escriben en el archivo \$NX_ROOT/NX.env. Para obtener más información acerca de las opciones de LDAP y las instrucciones para instalarlas, consulte la *ayuda en línea*.

2. Reinicie el servicio de CA Service Desk Manager.
Los cambios se aplican.

Opción	Valor predeterminado	Descripción
default_ldap_tenant		Necesario para la instalación de multicliente. Especifica la asignación de cliente predeterminada para los contactos importados de LDAP. Debe usar el UUID del cliente cuando establece el campo Valor de opción. Nota: Puede obtener el UUID del cliente a partir de una consulta de la base de datos. Por ejemplo, "SELECT * FROM ca_tenant".
ldap_enable	Sí	Obligatorio. Habilita la integración de LDAP con CA Service Desk Manager.
ldap_host		Obligatorio. Especifica el nombre de host o la dirección IP del servidor de base de datos LDAP.
ldap_port	389	Obligatorio. Especifica el número de puerto del servidor LDAP.
ldap_dn		Obligatorio. Especifica el nombre completo de inicio de sesión en el servidor LDAP. Por ejemplo: CN=Joe, CN=Users, DC=KLAND, DC=AD, DC=com Si el servidor LDAP admite enlaces anónimos, este valor se puede dejar en blanco.
ldap_pwd		Obligatorio. Especifica la contraseña para el nombre completo de inicio de sesión en el servidor LDAP. Si el servidor LDAP admite enlaces anónimos, este valor se puede dejar en blanco.
ldap_search_base		Obligatorio. Especifica el punto de partida para las búsquedas en el árbol del esquema LDAP: (UNIX) Debe especificar un contenedor de inicio. Por ejemplo: CN=Users, DC=KLAND, DC=AD, DC=com (Windows) No es necesario especificar un contenedor. Puede fijar el inicio en lo más alto del árbol del esquema. Por ejemplo: DC=KLAND, DC=AD, DC=com
ldap_filter_prefix	(&(objectClass=user)	Especifica el prefijo que se aplica a los filtros de generación automática cuando se buscan usuarios LDAP. Nota: Esta variable se ha sustituido por la opción

Opción	Valor predeterminado	Descripción
		ldap_user_object_class. No está disponible en el gestor de opciones, pero se puede definir manualmente en el archivo NX.env.
ldap_filter_suffix	)	Especifica el sufijo que se aplica a los filtros de generación automática cuando se buscan usuarios LDAP. Nota: Esta variable se ha sustituido por la opción ldap_user_object_class. No está disponible en el gestor de opciones, pero se puede definir manualmente en el archivo NX.env.
ldap_user_object_clase	person	Obligatorio. Especifica el valor del atributo LDAP objectClass que se aplica a un filtro de generación automática cuando se buscan usuarios LDAP.
ldap_enable_group	Sí	Opcional. Habilita la asignación del tipo de acceso de CA Service Desk Manager basada en pertenencia a grupos LDAP.
ldap_group_object_clase	grupo	Necesario solamente si ldap_enable_group está instalado. Especifica el nombre de objeto que se aplica a los filtros de generación automática cuando se buscan grupos.
ldap_group_filter_prefijo	(&(objectClass=group)	Especifica el prefijo que se aplica a los filtros de generación automática cuando se buscan grupos LDAP. Nota: Esta variable se ha sustituido por la opción ldap_group_object_class. No está disponible en el gestor de opciones, pero se puede definir manualmente en el archivo NX.env.
ldap_group_filter_sufijo	)	Especifica el sufijo que se aplica a los filtros de generación automática cuando se buscan grupos LDAP. Nota: Esta variable se ha sustituido por la opción ldap_group_object_class. No está disponible en el gestor de opciones, pero se puede definir manualmente en el archivo NX.env.
ldap_enable_auto	Sí	Opcional. Habilita la generación automática de registros de contacto de datos LDAP.
ldap_sync_on_null	Sí	Opcional. Sobrescribe los atributos de contacto de CA Service Desk Manager existentes con datos nulos si el atributo de usuario LDAP correspondiente contiene un valor nulo.

Opción	Valor predeterminado	Descripción
ldap_service_type	Active Directory	Opcional. Utilice esta opción si el entorno operativo de CA Service Desk Manager es Windows y el directorio LDAP <i>no</i> es Active Directory (es, por ejemplo, eTrust o Novell). Nota: En el entorno operativo UNIX, la funcionalidad "No AD" se utiliza sólo si esta opción <i>no</i> está instalada. Si se instala, el tipo de servicio se establece en Active Directory.
ldap_enable_tls	No	Opcional. Especifica si está activado Transport Layer Security (TLS) durante el procesamiento de LDAP.

Verificación de la integración de LDAP

Después de que haya instalado las opciones de LDAP necesarias, los usuarios de CA Service Desk Manager pueden importar los datos LDAP en forma individual y eliminar la necesidad de rellenar todos los campos de atributo de contacto en forma manual.

Para verificar que la integración de LDAP esté configurada correctamente, realice los siguientes pasos con la interfaz Web. Si encuentra problemas, consulte la Solución de problemas (see page 222).

Procedimiento para verificar que puede buscar e importar registros LDAP

1. Seleccione Archivo, Nuevo contacto de LDAP en la ficha Service Desk.
Aparece la ventana Búsqueda de directorios LDAP.
2. Especifique los criterios de filtrado y haga clic en Buscar. Por ejemplo, puede introducir b% en el campo Apellido para recuperar una lista de entradas de usuario de LDAP con los apellidos que empiecen por la letra B.

Nota: Si el directorio LDAP contiene miles de entradas y no se filtran las búsquedas, la solicitud intenta recuperar *todos* los registros de usuarios de LDAP. Esto puede ocasionar que la solicitud finalice y devuelva cero registros.

Se muestran los resultados de la búsqueda que coinciden con los criterios de filtrado.

3. Seleccione una entrada.

Aparece la ventana Crear nuevo contacto con los valores de los atributos LDAP importados.

4. Haga clic en Guardar.

Se crea el registro de contacto.

Procedimiento para verificar que puede actualizar un contacto con los datos LDAP

Nota: Antes de realizar este procedimiento, para fines de prueba, es posible que desee utilizar cualquier herramienta de edición de LDAP que tenga disponible para cambiar uno o más valores de los atributos en la entrada que usó para el procedimiento anterior. Puede comprobar si el contacto se ha actualizado con los datos LDAP más recientes.

1. Seleccione Buscar, Contactos en la ficha Service Desk.

Aparece la ventana Búsqueda de contactos.

2. Especifique los criterios de filtrado para buscar un contacto que tenga una entrada de usuario LDAP correspondiente. Por ejemplo, podría buscar el contacto que creó en el procedimiento anterior.

Se muestran los resultados de la búsqueda que coinciden con los criterios de filtrado.

3. Seleccione el contacto que desea actualizar con los datos LDAP.

La página Detalles de contacto aparece con la información de contacto de CA Service Desk Manager.

4. Haga clic en Editar.

Aparecerá la página Actualización de contactos.

5. Haga clic en Combinar LDAP.

La página Lista de entradas LDAP muestra una lista de algunas entradas de usuarios LDAP que corresponden al contacto de CA Service Desk Manager seleccionado.

Para buscar el directorio LDAP para otras entradas, haga clic en Mostrar filtro, especifique los criterios de filtrado y haga clic en Buscar.

Nota: Si el directorio LDAP contiene miles de entradas y no se filtran las búsquedas, la solicitud intenta recuperar *todos* los registros de usuarios de LDAP. Esto puede ocasionar que la solicitud finalice y devuelva cero registros.

6. Haga clic en la entrada LDAP que desee.

La página Detalles de LDAP muestra los valores de atributo para la entrada seleccionada. Verifique que ha seleccionado la entrada correcta para el contacto que desea actualizar y haga clic en Cerrar ventana.

7. En la página Lista de entradas LDAP, haga clic con el botón secundario en la entrada que mejor coincida con el contacto que desea actualizar y seleccione Combinar en contacto.

Vuelve a aparecer la página Actualización de contactos con los valores de los atributos LDAP actuales. Si los datos LDAP han cambiado desde que creó o actualizó por última vez el contacto, los cambios se reflejan en los campos de atributos de contacto.

Nota: Si ha instalado la opción `ldap_sync_on_null` y la entrada LDAP contiene valores nulos para algunos campos de atributo que corresponden a los atributos de contacto que actualmente contienen valores, los valores del registro de contacto se sobrescribirán con valores nulos cuando guarde los datos de contacto.

8. Haga clic en Guardar en la página Actualización de contactos.
El contacto se actualiza con los datos LDAP correspondientes.

Creación automática de un contacto

Puede configurar CA Service Desk Manager para crear en forma automática un contacto de un registro de usuarios LDAP correspondiente cuando un usuario nuevo inicia sesión en CA Service Desk Manager.

Para activar esta función, instale todas las opciones obligatorias de LDAP más la opción `ldap_enable_auto`.

El registro de contacto se crea automáticamente de la siguiente manera:

1. Si un usuario que inicia sesión en CA Service Desk Manager no tiene todavía un registro de contacto, pero el nombre de inicio de sesión del usuario existe en un registro LDAP, los datos LDAP se importan en forma automática y se crea un registro de contacto.
2. El registro de contacto creado en forma automática hereda la configuración de seguridad del tipo de acceso predeterminado.
3. Se le puede asignar al contacto un tipo de acceso en forma explícita o se puede asignar el tipo de acceso en función de la pertenencia del usuario a los grupos LDAP.

El usuario no percibe este proceso, que se produce como cualquier otro inicio de sesión.

Asignaciones del tipo de acceso de los grupos LDAP

Puede configurar CA Service Desk Manager para que asigne automáticamente valores de tipo de acceso a contactos en función de la pertenencia a grupos LDAP. Con la asignación de tipo de acceso automática habilitada, si un registro de usuario LDAP que se usó para crear un contacto pertenece a un grupo LDAP que se asocia con uno de los tipos de acceso de CA Service Desk Manager, se le asigna automáticamente al contacto ese tipo de acceso. De lo contrario, el contacto hereda el tipo de acceso predeterminado.

Para habilitar la asignación de tipo de acceso automática, debe instalar las opciones `ldap_enable_group` y `ldap_group_object_class`.

Nota: Para obtener detalles acerca de cómo instalar las opciones necesarias y asociar grupos LDAP con tipos de acceso, consulte la *ayuda en línea*.

Importación por lotes de contactos mediante datos LDAP

Puede ejecutar la utilidad de línea de comandos `pdm_ldap_import` para crear contactos de CA Service Desk Manager por lotes mediante datos de LDAP.

Nota: Además de crear contactos, `pdm_ldap_import` actualiza los contactos existentes si no están sincronizados con sus entradas LDAP correspondientes. Puede utilizar el proceso por lotes `pdm_ldap_sync` para actualizar los contactos existentes, pero no para crear uno.

Las sintaxis de `pdm_ldap_import` es la siguiente:

```
pdm_ldap_import -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]
```

-l "*ldap_where_clause*"

Especifica los ID de usuario (`userid`) de los registros LDAP que se buscarán. Las variables de reemplazo se indican con el carácter '?'. Por ejemplo, para `userid = ?`. El valor predeterminado es `userid = ?`. En este caso especial, `id` se asigna al atributo de contacto `ldap_dn`.

-c "*contact_where_clause*"

(Opcional) Especifica cómo determinar si el registro de contacto ya existe. Si el registro de contacto no existe, se inserta un nuevo registro de contacto. Si el registro de contacto existe y no se sincroniza con los datos de LDAP actuales, el registro de contacto se actualiza.

-u "*userid*"

(Opcional) Especifica el nombre de inicio de sesión bajo el cual se ejecuta el programa `pdm_ldap_import`.

Nota: Puede utilizar caracteres comodines con `pdm_ldap_import` para especificar varios registros.

Ejemplos: importaciones por lote mediante datos de LDAP

En este ejemplo se importa un único registro LDAP para el ID de usuario jsmith11:

```
pdm_ldap_import -l "userid = 'jsmith11'"
```

En este ejemplo se importan todos los registros LDAP con un ID de usuario que empieza con la letra C:

```
pdm_ldap_import -l "userid = 'c%'"
```

En este ejemplo se importan todos los registros de usuarios de LDAP en el directorio:

```
pdm_ldap_import -l "userid = '%'"
```

Más información:

[Actualización por lotes de contactos mediante datos LDAP](#) (en la página 217)

Importación de contactos por lotes según la fecha y hora

Puede configurar la utilidad `pdm_ldap_import` para importar registros LDAP que se crearon antes o después de una fecha y una hora especificadas. Para habilitar esta funcionalidad, cree un archivo `ldap.mod` con el contenido siguiente:

```
OBJECT ldap {  
  ATTRIBUTES LDAP_Entry {  
    whenCreated whenCreated STRING ;  
  };  
};
```

Esto agrega el atributo *whenCreated* al objeto LDAP.

Las reglas de registros de filtrado que utilizan el atributo `whenCreated` son las siguientes:

- Utilice solamente el operador `>=` o `<=`.
- Especifique *todos* los caracteres para el valor de fecha/hora, incluido Z. Coloque un 0 en cualquier ubicación que no desee indicar explícitamente (por ejemplo, la hora del día).
- Coloque la especificación de fecha/hora en el inicio del filtro; no utilice 0 al inicio de la cadena.
- No incluya el siglo. Para, por ejemplo, especificar el año 2008, use 08.

Nota: Las comillas simples deben rodear el valor de fecha/hora.

Ejemplo: uso del atributo whenCreated para importar entradas LDAP

El ejemplo siguiente usa el atributo whenCreated para importar entradas LDAP creadas después del 11/03/08.

```
pdm_ldap_import -l "whenCreated >= '080312000000z'"
```

Ejemplo: uso del atributo whenCreated para buscar registros LDAP

El ejemplo siguiente utiliza el atributo whenCreated con pdm_ldap_test para buscar registros LDAP creados después del 11/03/08.

```
pdm_ldap_test.exe -f "whenCreated>=080312000000z" -a whenCreated
Starting ldap_test.exe...
LDAP Directory Type : active directory
Service Desk Platform : windows
Search Base : DC=kirklandsd,DC=ca,DC=com
Search Filter : (&(objectClass=person)(whenCreated>=080312000000z))
Administrator Username :
CN=Administrator,CN=Users,DC=kirklandsd,DC=ca,DC=com
Administrator Password : *****
LDAP Host : gecko.kirklandsd.ca.com
LDAP Port : 389
LDAP API Version : 3
DN: CN=aixmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
    whenCreated(17) (0): 20080312035327.0Z
DN: CN=hpmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
    whenCreated(17) (0): 20080312035425.0Z
DN: CN=sunmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
    whenCreated(17) (0): 20080312035726.0Z
3 Total LDAP records found...
```

Resumen de la importación por lotes y datos de registro

El comando pdm_ldap_import mantiene un registro detallado de toda la actividad de cada ejecución. Este archivo de registro (ldap_logging.0-n) está ubicado en el directorio \$NX_ROOT/log.

El siguiente ejemplo muestra los retornos de pdm_ldap_import de datos resumidos en la línea de comandos:

```
pdm_ldap_import Starting...
pdm_ldap_import Summary: Processed(21) Updated(1) No Matches(7) New Contacts(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_import Complete...
```

En la tabla siguiente se describen los datos de resumen.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.	Número	Descripción
Processed	21	El número total de entradas LDAP encontradas
Actualizado	1	El número de registros de contacto que se actualizaron porque la entrada LDAP correspondiente contenía información diferente
No Matches	7	El número de entradas LDAP sin registro de contacto correspondiente
New Contacts	11	El número de nuevos registros de contacto que se crearon según las entradas LDAP correspondientes
Multiple Matches	0	El número de entradas LDAP con varios registros de contacto coincidentes, según lo definido en la opción ldap_search_base
Empty Filter	2	El número total de entradas LDAP que no sirven para generar filtros de búsqueda válidos
Errores	0	El número de entradas LDAP que han producido algún error durante el procesamiento. Por ejemplo, los registros LDAP que no contienen un valor en un campo requerido por CA Service Desk Manager (como el campo Apellido) se consideran erróneos y no se pueden importar.

Actualización por lotes de contactos mediante datos LDAP

Se puede ejecutar la utilidad `pdm_ldap_sync` para actualizar los registros de contacto por lotes mediante datos LDAP.

Importante: esta utilidad sobrescribe al cliente existente del contacto LDAP definido en CA Service Desk Manager. Si desea conservar el valor de cliente, debe modificar `NX.env`. Para ello, agregue manualmente la variable `NX_RETAIN_TENANT_VALUE` y configúrela en "sí". Si esta variable se configura en "no", no se encuentra, o no se configura correctamente, la utilidad sobrescribirá la información de cliente.

Nota: La utilidad `pdm_ldap_sync` sincroniza los contactos existentes con entradas LDAP correspondientes, pero no crea contactos. Puede utilizar el proceso por lotes `pdm_ldap_import` para crear contactos.

Las sintaxis de `pdm_ldap_sync` es la siguiente:

```
pdm_ldap_sync -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]
```

-l "*ldap_where_clause*"

Determina cómo buscar registros LDAP coincidentes. Las variables de reemplazo se indican con el carácter '?'. Por ejemplo, para `ID_usuario = ?`, `ID = ?` es el valor predeterminado. En este caso especial, `id` se asigna al atributo de contacto `ldap_dn`.

-c "*contact_where_clause*"

(Opcional) Determina que los contactos son utilizados al buscar registros LDAP coincidentes.

Predeterminado: "`ldap_dn IS NOT NULL`"

-u "*userid*"

(Opcional) Especifica el ID de usuario bajo el cual se ejecuta `pdm_ldap_sync`.

Nota: Puede utilizar caracteres comodines con `pdm_ldap_sync` para especificar varios registros.

Ejemplos:

Este ejemplo establece una línea base de registros de contacto que tienen un registro LDAP correspondiente:

```
pdm_ldap_sync -l "userid = ?" -c ""
```

Este ejemplo utiliza los parámetros predeterminados para actualizar todos los registros de contactos que posean un nombre completo para LDAP:

```
pdm_ldap_sync
```

Este ejemplo actualiza un solo contacto:

```
pdm_ldap_sync -l "userid = ?" -c "userid = 'jsmith11'"
```

Más información:

[Importación por lotes de contactos mediante datos LDAP](#) (en la página 213)

Resumen de la actualización por lotes y datos de registro

El comando `pdm_ldap_sync` conserva un registro detallado de todas las actividades de cada ejecución. El archivo `ldap_logging.0-n` está ubicado en el directorio `$NX_ROOT/log`.

A continuación se presenta un ejemplo de la devolución de datos de resumen `pdm_ldap_sync` en la línea de comandos:

```
pdm_ldap_sync Starting...
pdm_ldap_sync Summary:  Processed(21) Updated(1) No Matches(7) No Changes(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_sync Complete...
```

En la siguiente tabla se describe el resumen de los datos:

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.	Número	Descripción
Processed	21	El número total de entradas LDAP encontradas
Actualizado	1	El número de entradas LDAP cuya información es diferente a la del registro de contacto de CA Service Desk Manager correspondiente
No Matches	7	El número de entradas LDAP sin un registro de contacto de CA Service Desk Manager correspondiente
No Changes	11	El número de entradas LDAP cuya información es idéntica a la del registro de contacto de CA Service Desk Manager correspondiente
Multiple Matches	0	El número de entradas LDAP que presentan varios registros de contacto de CA Service Desk Manager coincidentes, según se define en la opción <code>ldap_search_base</code>

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.	Número	Descripción
Empty Filter	2	El número total de entradas LDAP que no sirven para generar filtros de búsqueda válidos
Errores	0	El número de entradas LDAP en las que se ha producido algún error durante el procesamiento

Autenticación LDAP

Se puede usar el protocolo LDAP para autenticar a los usuarios que inician una sesión en CA Service Desk Manager. La autenticación LDAP está disponible cuando el componente de autenticación de CA EEM se integra con CA Service Desk Manager, lo que reemplaza la validación predeterminada que ejecuta el sistema operativo del host. La autenticación LDAP sólo se puede aplicar si se ha configurado CA EEM para que utilice un directorio LDAP externo y se ha seleccionado la autenticación del sistema operativo como tipo de validación del usuario en un registro de tipo de acceso.

Cuando se activa una función de CA EEM, las solicitudes de inicio de sesión se comprueban con el servidor de CA EEM. Una solicitud de inicio de sesión se concede solamente si se produce alguna de las siguientes situaciones:

- La ID de usuario especificada coincide con un registro de contacto de CA Service Desk Manager.
- La ID del usuario coincide con un perfil de usuario de CA EEM.
- CA EEM valida correctamente la combinación de ID de usuario y contraseña.

Nota: Para obtener más información acerca de la utilización de CA EEM para realizar la autenticación, consulte la *Guía de implementación*. Para obtener más información sobre cómo configurar los tipos de acceso, consulte la *ayuda en línea*.

Transport Layer Security (seguridad de la capa de transporte)

Puede configurar CA Service Desk Manager para utilizar Transport Layer Security (TLS) durante el procesamiento de LDAP. TLS, un protocolo de comunicaciones seguras, es el sucesor del protocolo de seguridad Secure Socket Layer (SSL v3). Debe instalar la opción `ldap_enable_tls` para habilitar el protocolo TLS.

Importante: si se habilita esta opción, se codifican todas las comunicaciones entre CA Service Desk Manager y el servidor LDAP. Si *no* se habilita esta opción, todas las comunicaciones de datos (incluido el inicio de sesión administrativo y la contraseña utilizada para acceder al servidor LDAP) se envían en texto no cifrado.

Nota: Para obtener más información sobre cómo configurar TLS, consulte la documentación del servidor LDAP y del sistema operativo. Para obtener más información sobre cómo utilizar la opción `ldap_enable_tls`, consulte la *ayuda en línea*.

Asignación de atributos

Los valores de atributo de registro de contacto de CA Service Desk Manager se sincronizan con los valores de atributo de usuario de LDAP basados en las definiciones de asignación de atributos en el archivo `$NX_ROOT/bopcfg/majic/ldap.maj`.

El extracto siguiente de `ldap.maj` ilustra la asignación. Los nombres de atributo de la columna izquierda (`id`) son los nombres de atributo de contacto de CA Service Desk Manager. La columna del centro (`distinguishedName`) contiene los nombres de atributo de LDAP correspondientes.

<code>id</code>	<code>distinguishedName</code>	<code>STRING 512;</code>
<code>last_name</code>	<code>sn,pzLastName</code>	<code>STRING ;</code>
<code>first_name</code>	<code>givenName,pzFirstName</code>	<code>STRING ;</code>
<code>middle_name</code>	<code>initials,pzMiddleName</code>	<code>STRING ;</code>
<code>userid</code>	<code>uid,sAMAccountName,pzUserName</code>	<code>STRING ;</code>
<code>phone_number</code>	<code>telephoneNumber,pzworkPhoneNumber</code>	<code>STRING ;</code>

Si existe un SREL (una sola relación o la clave externa de otra tabla de la base de datos) en CA Service Desk Manager, el valor de atributo del contacto se sincronizará con el valor de LDAP correspondiente. Si el SREL no existe aún, no se creará automáticamente durante el proceso de sincronización de LDAP.

Nota: De forma predeterminada, se configura la asignación de atributos para el esquema de LDAP de Microsoft Active Directory. Si es necesario, puede cambiar la asignación mediante un archivo `mod`.

Cómo modificar la asignación de atributos

Puede cambiar la asignación de atributos predeterminada.

Para cambiar la asignación de atributos predeterminada, realice los pasos siguientes:

1. Desplácese a `$NX_ROOT/site/mods/majic` y abra el archivo `mod`.
2. Use las instrucciones `MODIFY` del archivo `mod` como se indica a continuación.
 - Las instrucciones `MODIFY` deben ser siempre las primeras del archivo.
 - Tras las instrucciones `MODIFY`, debe indicarse cualquier campo adicional que no esté en el archivo `ldap.maj` con la sintaxis que se muestra en el siguiente ejemplo.
 - Si define un campo que contiene un carácter de guión en el nombre de atributo, el nombre debe ir entre comillas sencillas; en caso contrario, cuando cree el archivo `mod`, el atributo fallará debido a un error de sintaxis. Por ejemplo, el siguiente nombre de atributo debe ir entre comillas sencillas:

```
c_nx_string1 'swsd-secret-question' STRING ;
```

3. Guarde y cierre el archivo `mod`.
4. Reinicie el servicio de CA Service Desk Manager.

Importante: el motor Web no se iniciará si hay una discrepancia en la sintaxis o en el uso de mayúsculas y minúsculas.

Sus cambios se aplicarán.

Ejemplo: utilización de instrucciones `MODIFY`

El ejemplo siguiente muestra cómo modificar dos campos y agregar otro.

```
//  
// Map CA Service Desk Manager userid attribute to ADAM UserId  
//  
MODIFY ldap userid cn ;  
MODIFY ldap middle_name middleName ;  
OBJECT ldap LDAP {  
  ATTRIBUTES LDAP_Entry{  
    contact_num employeeNumber STRING ;  
  };  
};
```

Solución de problemas

La principal consideración que se debe tener en cuenta al solucionar los problemas de comunicación de los servidores LDAP consiste en reconocer que rara vez existen dos implementaciones de LDAP idénticas. Las utilidades de CA Service Desk Manager pueden comprobar si la integración de LDAP funciona correctamente.

Nota: CA Service Desk Manager se preconfigura para la integración con Active Directory de Microsoft, eTrust e iPlanet solamente. La integración con otros servidores LDAP suele exigir la aplicación de cambios y ajustes a ambos lados.

Visualización del estado de los daemons o los procesos

El proceso ldap_virtldb gestiona las interacciones entre CA Service Desk Manager y la base de datos virtual de LDAP.

Procedimiento para ver el estado de todos los daemons (UNIX) o los procesos de CA Service Desk Manager

1. Ejecute pdm_status en la línea de comandos sin parámetros:

```
pdm_status
```

El comando pdm_status muestra el estado de todos los daemons (UNIX) o procesos (Windows) de CA Service Desk Manager del sistema en el que se ejecuta el comando. Por ejemplo:

DAEMON		STATUS	HOST	PID	SLUMP	CONNECT	TIME

--							
Agent antfarm		Running	antfarm	455	Tue	Feb	17
17:55:12							
Ddict_rd	(ddictrd)	Completed	antfarm				
Data Dictionary	(ddictbuild)	Completed	antfarm				
...							
User Validation	(boplgln)	Running	antfarm	456	Tue	Feb	17
17:55:21							

2. Examine el resultado del comando para ver el estado del proceso ldap_virtldb.

Comando slstat

Para verificar que bopLDAP esté conectado, ejecute el siguiente comando sin parámetros:

```
slstat
```

Examine el resultado del comando para ver el estado de bopLDAP.

Archivo NX.env

Revise el archivo `$NX_ROOT/NX.env` para comprobar que se hayan instalado correctamente las opciones de LDAP básicas.

Según qué opciones de LDAP se instalen, el archivo `NX.env` debería incluir líneas similares a las siguientes:

```
@NX_LDAP_DN=qouser
@NX_LDAP_ENABLE=Yes
@NX_LDAP_ENABLE_AUTO=Yes
@NX_LDAP_HOST=myserver
@NX_LDAP_PORT=389
@NX_LDAP_PWD=OBUNQxo7CmgbThZlCiMKIwJlA3UXdVNA0jupHjstfdt2LBIDPgwtWA==
@NX_LDAP_SEARCH_BASE=dc=mycontroller, dc=xyz, dc=com
@NX_LDAP_SERVICE_TYPE=Active Directory
@NX_LDAP_SYNC_ON_NULL=Yes
@NX_LDAP_USER_OBJECT_CLASS=person
```

Importante: dado que el servidor de directorio SunOne y los servidores eDirectory de Novell no admiten la búsqueda paginada, la búsqueda, importación y sincronización de LDAP se limitan al valor de los registros `NX_LDAP_MAX_FETCH` por invocación. El valor predeterminado es 100. Si está utilizando cualquiera de esos servidores LDAP, posiblemente desee agregar `NX_LDAP_MAX_FETCH` al archivo `NX.env` para especificar la cantidad máxima de registros LDAP. Puede establecer `NX_LDAP_MAX_FETCH` en cualquier valor menor al valor de `LDAP_SIZELIMIT_EXCEEDED` o `LDAP_ADMINLIMIT_EXCEEDED` en el servidor LDAP.

pdm_ldap_test

Use la utilidad de línea de comandos `pdm_ldap_test` para probar la conexión a un directorio LDAP, asegurarse de que las opciones de búsqueda estén configuradas correctamente y probar la configuración de TLS.

De forma predeterminada, `pdm_ldap_test` utiliza los valores de configuración de los parámetros que se introducen en el archivo `$NX_ROOT/NX.env` cuando se instalan, editan o desinstalan opciones de LDAP. Para sustituir los valores predeterminados, puede especificar los parámetros en la línea de comandos `pdm_ldap_test`.

Para ver los parámetros disponibles para este comando, introduzca el siguiente comando:

```
pdm_ldap_test -h
```

Importante: En UNIX, `LIBPATH` debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice `pdm_task` para definir `LIBPATH` antes de ejecutar una utilidad. Por ejemplo, indique "`pdm_task pdm_clean_attachments ...`".

Comprobación de la conexión al servidor LDAP

Para comprobar la conexión al servidor LDAP, ejecute `pdm_ldap_test` sin parámetros:

```
pdm_ldap_test
```

Conexión correcta al servidor LDAP

Si la conexión se establece con éxito, se obtiene un resultado similar al siguiente:

```
Iniciando pdm_ldap_test ...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Correcto)
ldap_bind_s(Administrator) (Success)
LDAP API Verion 3
```

Error de conexión: servidor sin servicio o nombre o puerto incorrecto

Si se produce un error de conexión porque el servidor se encuentra sin servicio o porque el nombre o el puerto especificado para el servidor LDAP no es correcto, se obtiene un resultado similar al siguiente:

```
Iniciando pdm_ldap_test ...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(junk,389): (Success)
ldap_bind_s(Administrator) (Server Down)
```

Error de conexión: LDAP_DN o LDAP_PWD no válido

Si se produce un error de conexión porque el LDAP_DN o LDAP_PWD especificado es incorrecto, se obtiene un resultado similar al siguiente:

```
Iniciando pdm_ldap_test ...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Correcto)
ldap_bind_s(junk) (No Such Object or Invalid Credentials)
```


Consulta de parámetros de búsqueda

Para comprobar que los parámetros de búsqueda estén configurados correctamente, ejecute `pdm_ldap_test` sin parámetros:

```
pdm_ldap_test
```

Búsqueda correcta

Si la búsqueda se realiza con éxito, se obtiene un resultado similar al siguiente:

```
DN: CN=Paul b. Gordon,CN=Users,DC=USVDTEST
    c(2)(0): US
    displayName(14)(0): B de Paul. Gordon
    mail(14)(0): gorpa02@ca.com
    givenName(4)(0): Paul
    initials(1)(0): b
    distinguishedName(38)(0): CN=Paul b.
Gordon,CN=Users,DC=USVDTEST
    objectGUID(3)(0): 314738
    pager(12)(0): 516-647-1111
    postalCode(5)(0): 11111
    SAMAccountName(7)(0): gorpa02
    sn(6)(0): Gordon
    telephoneNumber(12)(0): 631-342-6265
    userPrincipalName(16)(0): gorpa02@USVDTEST

DN: CN=mike Habek,CN=Users,DC=USVDTEST
    displayName(10)(0): mike Habek
    givenName(4)(0): mike
    distinguishedName(34)(0): CN=mike
Habek,CN=Users,DC=USVDTEST
    objectGUID(12)(0): 312328
    SAMAccountName(7)(0): habmi02
    sn(5)(0): Habek
    userPrincipalName(16)(0): habmi02@USVDTEST
```

Error de búsqueda: SEARCH_BASE no válido

Si se produce un error de búsqueda debido a que SEARCH_BASE no es válido, se obtiene un resultado similar al siguiente:

```
Iniciando pdm_ldap_test ...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Correcto)

ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() (No Such Object or Referral)
```

Error de búsqueda: SIZELIMIT_EXCEEDED y TIMEOUT

La búsqueda puede no terminar correctamente y mostrar un mensaje de error SIZELIMIT_EXCEEDED o TIMEOUT si el filtro especificado no la acota lo suficiente. La mayoría de los servidores LDAP limita el tamaño del conjunto de resultados que se devuelven en las solicitudes de búsqueda. Cuando se sobrepasa este límite, aparecerá un mensaje SIZELIMIT_EXCEEDED. Si la solicitud de búsqueda tarda más de 20 segundos, el tiempo de espera predeterminado, el servidor LDAP da por agotado su tiempo y aparece un mensaje de error TIMEOUT parecido al siguiente:

```
Iniciando pdm_ldap_test ...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Correcto)
ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() (TIMEOUT or SIZELIMIT_EXCEEDED)
```

Error de búsqueda: ningún registro devuelto

En ocasiones, se producen errores en las búsquedas porque el filtro predeterminado no es correcto. Si `pdm_ldap_test` no devuelve ningún registro (0), se debe comprobar siempre la línea "Using filter", que es el filtro base que generan las opciones `LDAP_FILTER_PREFIX` y `LDAP_FILTER_SUFFIX` o la opción `LDAP_OBJECT_CLASS`:

```

Iniciando pdm_ldap_test ...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabs
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Correcto)
ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() 0 records

```

Acotamiento de búsquedas

Utilice el parámetro `-f` con el comando `pdm_ldap_test` para especificar el filtro que se va a agregar al filtro base con el fin de restringir los criterios de búsqueda. En el filtro se deben utilizar tanto la sintaxis LDAP apropiada como los nombres de atributos del esquema LDAP adecuados. Encierre los filtros entre comillas dobles y use paréntesis para aclarar el orden de prioridad de los operadores.

Por ejemplo, use el siguiente comando para buscar todos los registros en los que aparece `sn=Account_10001`:

```
pdm_ldap_test -f "(sn=Account_10001)"
```

La utilidad `pdm_ldap_test` admite los siguientes operadores de igualdad:

Operador de igualdad	Descripción
=	igual a
<=	menor que o igual a
>=	mayor que o igual a
~=	como

La utilidad `pdm_ldap_test` admite los siguientes operadores booleanos:

Operador booleano	Descripción
&	Y

Operador booleano	Descripción
	O
!	NO

Los operadores Y y O afectan a todos los conjuntos de paréntesis () del filtro de búsqueda. El NO sólo afecta al primer conjunto de paréntesis. Coloque estos operadores siempre *antes* de los filtros de búsqueda a los que se aplican en lugar de colocarlos en el medio de ellos. Estos operadores se pueden aplicar a cuantos filtros se desee, como se muestra en el siguiente ejemplo:

```
"(&(sn=Brown)(initials=A))"
```

```
"(|(sn=Brown)(sn=Smith))"
```

```
"(!sn=Brown)"
```

Determinación de los nombres de atributos que poseen valores

Utilice los parámetros -a "*" y -f con el comando `pdm_ldap_test` para determinar qué atributos se han definido para los registros de grupos y usuarios LDAP. Esta prueba resulta de utilidad para ver si existe algún atributo LDAP que desee asignar a los atributos de contacto, y para verificar si un atributo determinado dispone de un valor y debe estar disponible al crear o actualizar los registros de contacto.

En este ejemplo se muestra el resultado de un directorio iPlanet:

```
pdm_ldap_test -a "*" -f sn=Account_1000001

2 LDAP records found...

DN: cn=Account_1000001,ou=200K_Plus,o=SmartLabs
    sn(15)(0): Account_1000001
    objectClass(13)(0): inetOrgPerson
    objectClass(20)(1): organizationalPerson
    objectClass(6)(2): person
    objectClass(18)(3): ndsLoginProperties
    objectClass(3)(4): top

DN: cn=Account_1000001,ou=2_Plus,o=SmartLabs
    mail(28)(0): ThisIsTheMailingAddressField
    uid(13)(0): Login_1000001
    givenName(17)(0): GivenNameOfPerson
    sn(15)(0): Account_1000001
    objectClass(13)(0): inetOrgPerson
    objectClass(20)(1): organizationalPerson
    objectClass(6)(2): person
    objectClass(18)(3): ndsLoginProperties
    objectClass(3)(4): top
```

En este ejemplo se muestra el resultado de Active Directory:

```
Ldap_test -a "*" -f (&(sn=Brown)(initials=A))"
```

1 LDAP records found...

```
DN: CN=John A. Pérez,CN=Users,DC=mycontroller,DC=xyz,DC=com
  objectClass(3)(0): top
  objectClass(6)(1): person
  objectClass(20)(2): organizationalPerson
  objectClass(4)(3): user
  cn(16)(0): John A. Smith
  sn(5)(0): Brown
  givenName(7)(0): John
  initials(1)(0): A
  distinguishedName(55)(0): CN=John A.
  Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
  displayName(16)(0): John A. Smith
  memberOf(52)(0): CN=Domain Admins,CN=Users,DC=mycontroller,DC=xyz,DC=com
  sAMAccountName(7)(0): smijo04
  userPrincipalName(25)(0): smijo04@mydomain.xyz.com
  objectCategory(63)(0):
  CN=Person,CN=Schema,CN=Configuration,DC=mycontroller,DC=xyz,DC=com
```

Activación del seguimiento de LDAP

La utilidad `pdm_logstat` permite activar el registro de seguimiento para la supervisión del uso de LDAP en CA Service Desk Manager.

El comando `pdm_logstat` presenta la siguiente sintaxis:

```
pdm_logstat -f ldap_virtldb.c 1000
```

Los siguientes mensajes del archivo `stdlog` ayudan a comprender el estado del proceso de conexión.

Determinación de si se ha iniciado el proceso `ldap_virtldb`

Al analizar el archivo `stdlog` en busca de mensajes de LDAP, la primera línea que se debe buscar es la del inicio del proceso `ldap_virtldb`. CA Service Desk Manager sólo reconoce la presencia de LDAP una vez iniciado este proceso.

Nota: Aunque no se hayan instalado ni configurado las opciones de integración de LDAP, este proceso se ejecuta de todos modos.

```
06/03 17:00:18.27 cpasdl bopLDAP 1964 SIGNIFICANT ldap_virtldb.c
680 STARTUP of LDAP_virtldb
```

Determinación de si están instaladas todas las opciones obligatorias

Si no se ha definido alguna de las opciones de LDAP obligatorias, el archivo `stdlog` muestra las que faltan como se ilustra en el siguiente ejemplo:

```
06/03 17:00:18.72 cpasdl bopLDAP 1964 SEVERE_ERROR ldap_virtddb.c 1023 LDAP
Server port id missing
06/03 17:00:18.78 cpasdl bopLDAP 1964 SEVERE_ERROR ldap_virtddb.c 1023 LDAP
Server distinguished name missing
06/03 17:00:18.78 cpasdl bopLDAP 1964 SEVERE_ERROR ldap_virtddb.c 1023 LDAP
Server distinguished name password missing
```

Determinación de si la conexión a LDAP es correcta

Para comprobar si la conexión a LDAP es correcta, basta con mirar las entradas del archivo `stdlog`. Las entradas deben indicar que la conexión al servidor LDAP se ha establecido correctamente como se ilustra en el siguiente ejemplo:

```
06/05 12:35:10.41 cpasdl bopLDAP 1912 SIGNIFICANT ldap_virtddb.c 958
LDAP_SRVR connecting to host(Francisco.us.danconia.net) port(389)
06/05 12:35:11.01 frisco bopLDAP 1912 SIGNIFICANT ldap_virtddb.c 1002
LDAP_SRVR binding with username(simon)
```

Determinación de si la conexión a LDAP no está disponible

Si existe algún motivo por el que no resulta posible establecer la conexión al servidor LDAP, las funciones de LDAP *Entradas LDAP*, *Combinar LDAP* o cualquier otra se desconectan y no devuelven ningún resultado. En estos casos, al acceder a dichas operaciones, el archivo `stdlog` muestra mensajes similares a los siguientes:

```
06/03 17:00:32.25 cpasdl bopLDAP 1964 SIGNIFICANT ldap_virtddb.c 219 LDAP
server not available; 'register_producer' not processed

06/05 10:52:57.63 cpasdl bopLDAP 1896 SIGNIFICANT ldap_virtddb.c 219 LDAP
server not available; 'select_full' not processed

06/05 10:52:57.66 cpasdl web:local 1868 ERROR sel_data_cache. 611 Error in
ldap Select_Cache method got_initial_count: LDAP server not available;
'select_full' not processed

06/05 10:52:57.66 cpasdl bopLDAP 1896 SIGNIFICANT ldap_virtddb.c 219 LDAP
server not available; 'select_cancel' not processed
```

Determinación del filtro utilizado

CA Service Desk Manager busca registros de los directorios LDAP de acuerdo con la base de búsqueda y el filtro definidos en el gestor de opciones así como con los criterios de búsqueda especificados por el usuario. Localice el siguiente mensaje para determinar el filtro generado en la solicitud de búsqueda:

```
06/24 14:18:28.32 mcxxx04- bopLDAP      3844 TRACE    ldap_virtddb.c    853 Starting
select full: base=DC=kirklandsd,DC=ca,DC=com;
filter=(&(objectCategory=person)(|(sn=Jones)(pzLastName=Jones)));
attributes=(uid,SAMAccountName,pzUserName,distinguishedName)
```

Determinación de atributos buscados

CA Service Desk Manager busca registros de los directorios LDAP de acuerdo con la base de búsqueda y el filtro definidos en el gestor de opciones. Localice el mensaje siguiente para determinar si SEARCH_BASE y la asignación de atributos definidos en ldap.maj y ldap_group.maj son correctos:

```
06/24 14:18:28.39 mcxxx04- bopLDAP      3844 TRACE    ldap_virtddb.c    766
Starting select short: base=CN=John D. Jones,CN=Users,DC=kirklandsd,DC=ca,DC=com;
filter=(&(objectCategory=person));
attributes=(modifyTimestamp,sn,pzLastName,givenName,pzFirstName,initials,pzMiddle
Name,uid,SAMAccountName,pzUserName,telephoneNumber,pzworkPhoneNumber,mobile,pzMob
ilePhoneNumber,department,pzDepartment,facsimileTelephoneNumber,pzFaxPhoneNumber,
pager,mail,pzEmailAddress,streetAddress,pzAddress,1,pzCity,st,pzState,postalCode,
pzPostalCode,c,pzCountry,o,memberOf)
```

Determinación de datos LDAP disponibles y no disponibles

Si CA Service Desk Manager es capaz de asignar los atributos de ID de los objetos LDAP correctamente, se recuperan los atributos definidos en \$NX_ROOT/bopcfg/majic/ldap.maj para cada una de las entradas; o bien, se registra un mensaje que indica que no se ha definido ningún atributo. A continuación figura un ejemplo de estos mensajes:

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE    ldap_virtddb.c    1396 value
not available for 'modifyTimestamp'
```

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE    ldap_virtddb.c    1396 value
not available for 'telephoneNumber,pzworkPhoneNumber'
```


Capítulo 6: Gestión de roles

Nota: Para obtener más información sobre otros aspectos de la interfaz Web, consulte Configuración de la interfaz Web (see page 363).

Esta sección contiene los siguientes temas:

[Funciones](#) (en la página 233)
[Roles predefinidos](#) (en la página 233)
[Seguridad basada en roles](#) (en la página 236)
[Navegación basada en roles](#) (en la página 245)
[Cómo implementar un rol personalizado](#) (en la página 254)
[Cómo implementar un árbol de menús personalizado](#) (en la página 256)
[Creación de un registro de rol](#) (en la página 257)
[Creación de un registro de ficha](#) (en la página 258)
[Creación de un registro de barra de menús](#) (en la página 259)
[Creación de registros de formularios Web](#) (en la página 260)
[Cómo copiar árboles de menús](#) (en la página 261)
[Cómo crear y personalizar un árbol de menús](#) (en la página 262)
[Creación y publicación de un conjunto de ayuda](#) (en la página 264)
[Cambio de roles](#) (en la página 265)

Funciones

Los *roles* son los registros principales que controlan la navegación por la interfaz de usuario y la seguridad de CA Service Desk Manager. Cada rol define una vista específica del sistema exponiendo sólo las funciones necesarias para que los usuarios realicen las tareas asignadas normalmente a la función que desempeñan dentro de su organización empresarial.

El rol predeterminado de un usuario determina la vista de sistema que se presenta al iniciar sesión. Los usuarios con varios roles asignados pueden pasar de un rol a otro para ver diferentes vistas del sistema sin necesidad de desconectarse e iniciar sesión de nuevo.

Roles predefinidos

Puede usar los roles predefinidos en la configuración predeterminada, modificarlos para satisfacer sus requisitos empresariales o para crear roles nuevos.

La siguiente tabla describe los roles predefinidos que se instalan junto con CA Service Desk Manager. Estos roles están diseñados para adaptarse a las prácticas recomendadas de ITIL v3, por lo que se reduce la cantidad de personalización específica del sitio necesaria para que la organización de TI cumpla los requisitos de ITIL.

CA Service Desk Manager admite solamente ITIL, y la documentación de CA Service Desk Manager está orientada a ITIL. Para obtener más información, consulte la sección Configuración de ITIL (see page 30).

Tipo de rol:	Nombre del rol	Descripción
Usuarios finales	Visor de configuración	Ejecuta tareas de visualización e investigación de CI básicas desde el interior de la organización.
	Cliente	Ejecuta tareas de autoservicio básicas desde el exterior de la organización.
	Empleado	Ejecuta tareas de autoservicio básicas desde el interior de la organización.
Analistas	Analista de configuración	Ejecuta tareas dentro del proceso de ciclo de vida del elemento de configuración y proporciona la segunda línea de soporte de CMDB dentro de la organización.
	Representante del servicio de atención al cliente	Brinda soporte a los usuarios externos a la organización, en su mayoría clientes.
	Analista de conocimiento	Ejecuta tareas dentro del proceso de ciclo de vida de gestión del conocimiento.
	Analista de nivel 1	Proporciona primera línea de soporte dentro de la organización.
	Analista de nivel 2	Proporciona la segunda línea de soporte dentro de la organización, que requiere experiencia más avanzada en la materia.
	Analista de Automatización de soporte	Proporciona la primera línea de soporte dentro del entorno de asistencia en vivo.
	Analista de distribuidores	Brinda soporte a un segmento limitado del entorno de TI desde afuera de la organización, como un hardware específico de un distribuidor.
Administradores	Gestor de cambios	Gestiona el proceso de órdenes de cambio, pero normalmente no es un rol que ocupen analistas que trabajan en los tickets de órdenes de cambio.

Tipo de rol:	Nombre del rol	Descripción
	Gestor de servicio al cliente	Gestiona a los representantes del servicio al cliente y el proceso de soporte externo.
	Gestor de incidentes	Gestiona el proceso de incidentes, pero normalmente no es un rol que ocupen analistas que trabajan en los tickets de incidentes.
	Gestor de conocimientos	Supervisa a los analistas de conocimiento, las reasignaciones y escalaciones de documentos de conocimiento, así como la gestión diaria de conocimiento.
	Gestor de problemas	Gestiona el proceso de problemas, pero normalmente no es un rol que ocupen analistas que trabajan en los tickets de problemas.
	Service Desk Manager	Se ocupa de las escalaciones y supervisa a los analistas de nivel 1. También puede gestionar las operaciones generales del centro de servicio al usuario.
Administradores	Administrador	Ejecuta tareas administrativas a lo largo de todo el proceso de implementación de CA Service Desk Manager y Gestión del conocimiento. Por lo general, este rol se ocupa de instalar, configurar e integrar los productos.
	Administrador de configuración	Ejecuta tareas administrativas relacionadas con la implementación de CA CMDB. Por lo general, este rol se ocupa de administrar la CMDB, así como la infraestructura del elemento de configuración y las estructuras de datos.
	Administrador de gestión del conocimiento	Determina y controla la configuración de la gestión del conocimiento.
	Administrador de Service Desk	Ejecuta tareas administrativas de datos y procesos, como la creación y actualización de categorías, contactos, tipos de servicios, causas raíz, etc.
	Administrador de Automatización de soporte	Ejecuta tareas administrativas relacionadas con el entorno de Automatización de soporte, como la configuración de colas y permisos para herramientas de análisis.
	Administrador del sistema	Ejecuta tareas administrativas relacionadas con la implementación, configuración y adaptación de CA Service Desk Manager, como determinar opciones, configurar integraciones y modificar formularios Web.

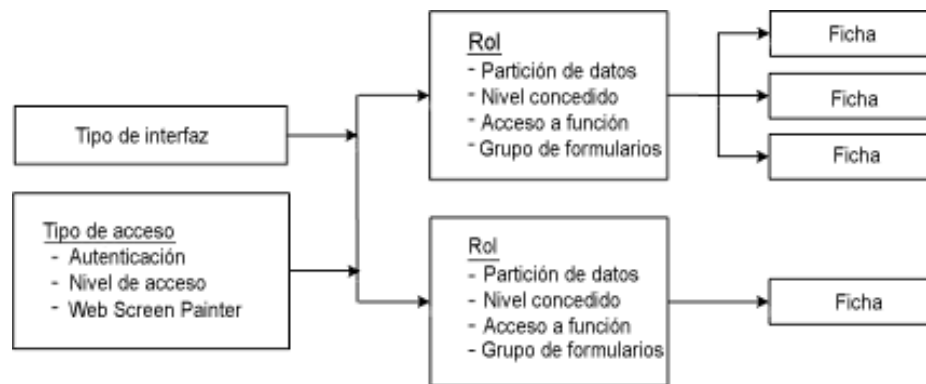
Tipo de rol:	Nombre del rol	Descripción
	Administrador de clientes	Ejecuta tareas administrativas multicliente específicas de un cliente u organización de soporte en particular.

Seguridad basada en roles

Los tipos de acceso y los roles son los principales componentes que se utilizan para controlar la seguridad de CA Service Desk Manager.

El siguiente diagrama muestra una descripción general de la forma en que los roles se relacionan con otros objetos del sistema para proporcionar seguridad basada en roles.

Nota: Para obtener más información sobre otros aspectos relacionados con la seguridad, consulte el tema Seguridad (see page 171).



Cómo funcionan los tipos de acceso

Cada tipo de acceso de un usuario controla los siguientes aspectos del comportamiento del sistema:

- Cómo realiza CA Service Desk Manager la autenticación de Web cuando el usuario inicia sesión.
- El nivel de acceso del usuario.
- Si el usuario puede modificar los formularios Web o el esquema de base de datos que utiliza Web Screen Painter.
- Qué roles están disponibles para el usuario.

Si desea asociar un tipo de acceso con un contacto, puede seleccionar el tipo de acceso durante la creación o actualización del registro de contacto.

La siguiente tabla enumera los tipos de acceso predefinidos, identifica sus roles relacionados y proporciona una descripción breve.

Tipo de acceso	Roles relacionados	Descripción
Administración	■ Administrador (predeterminado) ■ Administrador de configuración ■ Empleado ■ Analista de nivel 2 ■ Administrador de Service Desk ■ Administrador del sistema ■ Administrador de clientes	Proporciona el nivel máximo de acceso de seguridad a todos los roles clave de la administración. Se utiliza durante la implementación y la administración en curso. Nota: El tipo de acceso de administración se preconfigura para permitir que los administradores se cambien a cualquier rol relacionado. Por ejemplo, para obtener una vista diferente del sistema, los administradores pueden pasarse al rol de empleado sin necesidad de desconectarse y conectarse otra vez.
Cliente	■ Cliente	Proporciona acceso altamente restringido a los clientes <i>externos</i> que utilizan la vista de autoservicio.
Empleado	■ Empleado	Proporciona acceso altamente restringido a los empleados <i>internos</i> que utilizan la vista de autoservicio. Se utiliza para crear nuevos incidentes y páginas de actualización de incidentes.
Personal de TI	■ Analista de configuración ■ Empleado ■ Analista de nivel 2 (predeterminado) ■ Analista de conocimiento ■ Administrador de gestión del conocimiento ■ Gestor de conocimientos	Proporciona acceso de analista a los usuarios que trabajan dentro de la organización de TI, pero no son miembros reales del equipo de soporte. Este acceso está diseñado específicamente para usuarios que necesitan acceder a Gestión del conocimiento.
Gestión del conocimiento	■ Administrador de configuración ■ Analista de configuración ■ Visor de configuración ■ Empleado ■ Analista de conocimiento ■ Administrador de gestión	Proporciona acceso administrativo adaptado a los usuarios que administran funciones de Gestión del conocimiento.

Tipo de acceso	Roles relacionados	Descripción
	■ del conocimiento (predeterminado) ■ Gestor de conocimientos ■ Analista de nivel 2	
Gestión del proceso	■ Gestor de cambios ■ Analista de configuración ■ Empleado ■ Gestor de incidentes (predeterminado) ■ Analista de nivel 2 ■ Gestor de problemas ■ Service Desk Manager	Proporciona acceso adaptado a los usuarios que ejecutan roles clave de gestión del proceso.
Gestión de Service Desk	■ Gestor de servicio al cliente ■ Analista de configuración ■ Empleado ■ Analista de nivel 1 ■ Analista de nivel 2 ■ Gestor de Service Desk (predeterminado)	Proporciona acceso adaptado a los usuarios que gestionan el soporte de IT o las funciones del servicio de atención al cliente externo (por lo general, los supervisores de atención al cliente de primera línea).
Personal del centro de servicio al usuario	■ Analista de configuración ■ Visor de configuración ■ Representante del servicio de atención al cliente ■ Empleado ■ Analista de nivel 1 (predeterminado) ■ Analista de nivel 2	Proporciona acceso adaptado a los usuarios que ejecutan tareas de soporte. El acceso está dirigido a los usuarios que se ocupan de la atención al cliente de primera línea.
Administrador de Automatización de soporte	■ Administrador de Automatización de soporte	Proporciona acceso a los usuarios que se ocupan de la administración de Automatización de soporte.
Analista de Automatización de soporte	■ Analista de Automatización de soporte	Otorga acceso a los usuarios que proporcionan asistencia en vivo para los usuarios finales.
Personal de distribución	■ Analista de distribuidores	Proporciona acceso altamente restringido a los distribuidores externos que trabajan sólo sobre elementos directamente relacionados

Tipo de acceso	Roles relacionados	Descripción
		con su producto (por ejemplo, una marca particular de hardware).

Registros de rol

Puede asignar roles a un tipo de acceso o directamente al registro de contacto de un usuario. Si se produce un conflicto de asignación de roles, las asignaciones de roles de contacto tienen prioridad.

Cada registro de rol se debe configurar con los siguientes componentes:

- Un grupo de formularios
- Un tipo de interfaz de usuario
- Configuración de acceso a la función
- Una o más fichas
- Un conjunto de ayudas

Los siguientes componentes opcionales también pueden ayudar a definir cada rol:

- Árboles de menús
- Paneles de resultados
- Barras de menús
- Barras de herramientas
- Una partición de datos
- Acceso a Gestión del conocimiento
- Niveles de acceso a Automatización de soporte
- Formularios Web de informes
- Ir a recursos

Áreas de acceso funcional

Las áreas de acceso funcional definen el nivel de acceso por rol a los registros de ticket y otros componentes del sistema. La tabla `usp_functional_access_type` define el área y las tablas `usp_functional_access_level` describen el nivel de acceso del usuario.

La siguiente tabla muestra las áreas de acceso funcional predeterminadas:

Nombre	Nombre de código	Nuevo
Administración	admin	No
Incidente/problema/solicitud	call_mgr	No
Orden de cambios	change_mgr	No
Inventario	inventario	No
Incidencia	issue_mgr	No
Documento de conocimiento	KD	No
Notificación	notificar	No
Referencia	referencia	No
Seguridad	seguridad	No
Anuncio	anuncio	Sí
Referencia de incidente/problema/solicitud	call_mgr_reference	Sí
Plantilla de incidente/problema/solicitud	call_mgr_template	Sí
Plantilla de orden de cambio	change_mgr_template	Sí
Referencia de orden de cambio	change_reference	Sí
Elemento de configuración	ci	Sí
Elemento de configuración común sólo de lectura	ci_common_ro	Sí
Referencia del elemento de configuración	ci_reference	Sí
Contacto	contact	Sí
Group	grupo	Sí
Plantilla de incidencia	issue_mgr_template	Sí
Referencia de la incidencia	issue_reference	Sí
Ubicación	ubicación	Sí
Administración de varios sitios	multisite_admin	Sí
Referencia de varios sitios	multisite_reference	Sí
Referencia de notificación	notification_reference	Sí

Organization	organización	Sí
Fijación de prioridades	fijación de prioridades	Sí
Nivel de servicio	service_level	Sí
Departamento	site	Sí
Consulta almacenada	stored_queries	Sí
Automatización de soporte	sa	Sí
Estudio	estudio	Sí
Administrador de clientes	tenant_admin	Sí
Zona horaria	timezone	Sí
Referencia del workflow	workflow_reference	Sí
Turno	turnos	Sí

Cómo agregar un área de acceso funcional

Cuando agrega un área de acceso funcional, los roles existentes automáticamente tienen acceso para modificar. Puede revisar y cambiar los niveles de acceso para conceder la autoridad necesaria.

Para agregar un área de acceso funcional, realice lo siguiente:

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Acceso funcional.
2. Haga clic en Crear nuevo.
Aparecerá la página de lista Crear nuevo acceso funcional.
3. Rellene los campos de área de acceso funcional según corresponda.
4. Haga clic en Guardar.
Aparecerá la página Detalles de acceso funcional.
5. Aplique niveles de acceso a uno (see page 243) o más (see page 242) roles.

Nota: Para obtener información detallada sobre áreas de acceso funcional, vea la *Ayuda en línea*.

Aplicación de niveles de acceso a muchos roles

En el caso de un área de acceso funcional, puede establecer los niveles de acceso para que todos los roles ahorren tiempo. En lugar de usar Gestión de roles, puede actualizar el área de acceso funcional con los niveles de acceso de rol apropiados.

Para aplicar niveles de acceso a muchos roles, realice lo siguiente:

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Acceso funcional.
2. Haga clic en el nombre del área de función.
3. En la ficha Roles, haga clic en Editar en lista.
4. Revise y actualice cada rol según sea necesario. Están disponibles los siguientes niveles de acceso:

Ninguno

Deniega el acceso de rol al objeto de función.

Vista

Otorga capacidad de sólo lectura al objeto de función.

Modificar

Otorga acceso de lectura/escritura al objeto de función.

5. Continúe seleccionando roles y eligiendo niveles de acceso.
6. (Opcional) Haga clic en Cambiar todo.
7. Haga clic en Guardar.

Los cambios de los roles se aplican inmediatamente.

Nota: Para obtener información sobre roles y niveles de acceso funcional, consulte la *Ayuda en línea*.

Ejemplo: cambio de los niveles de acceso para el anuncio

En este ejemplo se muestra que puede cambiar los niveles de acceso de rol para el área de acceso funcional del anuncio.

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Acceso funcional.
Aparecerá la página Detalles de acceso funcional.
2. Haga clic en Anuncio.
3. En la ficha Roles, haga clic en Editar en lista.

4. Seleccione Analista de nivel 2.
5. Seleccione Ver en el Nivel de acceso.
El nivel de acceso para el analista de nivel 2 se resalta con el valor de vista.
6. Seleccione Analista de configuración.
7. Seleccione Modificar en el Nivel de acceso.
El nivel de acceso para el analista de configuración se resalta con el valor de vista.
8. Haga clic en Guardar.
Un mensaje confirma el cambio.
9. Inicie sesión con rol de analista de nivel 2.
10. Seleccione Ver anuncios.
Aparecerá la página Anuncios.
11. Haga clic en un anuncio.
Un mensaje le recuerda que como analista de nivel 2, sólo puede ver anuncios.
12. Establezca el rol en Analista de configuración.
13. Seleccione Ver anuncios.
Aparecerá la página Anuncios.
14. Haga clic en un anuncio.
Aparecerá la página Actualizar anuncio. Como analista de configuración, puede modificar anuncios.

Aplicación de un nivel de acceso para un rol

Puede utilizar la Gestión de roles para cambiar el modo de acceso de los usuarios a la interfaz de usuario. Cuando cambia los niveles de acceso para un rol, la interfaz de usuario sólo muestra objetos, páginas y elementos de menú con base en el nivel de acceso. Por ejemplo, si un rol ya no puede crear contactos, el menú Archivo omite nuevos contactos.

Para aplicar un nivel de acceso a un rol, realice lo siguiente:

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Gestión de roles, Lista de roles.
2. En la Lista de roles, haga clic con el botón secundario en el nombre de rol y seleccione Editar en el menú contextual.

3. En la ficha Acceso a la función, haga clic en Editar en Lista
4. Haga clic en el nombre de una función.
Se resalta la fila.
5. Actualice las áreas de acceso funcional con los siguientes niveles de acceso según sea necesario:

Ninguno

Deniega el acceso de rol al objeto de función.

Vista

Otorga capacidad de sólo lectura al objeto de función.

Modificar

Otorga acceso de lectura/escritura al objeto de función.

6. Haga clic en Guardar.
Un mensaje confirma el cambio. El rol puede utilizar inmediatamente el área de acceso funcional en el nivel de acceso especificado.
7. Para verificar el nivel de acceso, inicie sesión como el rol y compruebe los menús, las opciones de página y los botones.

Ejemplo: concesión de acceso para modificar tickets al rol de analista de nivel 2

Este ejemplo muestra cómo cambia la interfaz de usuario cuando se concede acceso para modificar tickets a un analista de nivel 2.

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Gestión de roles, Lista de roles.
Aparecerá la lista de roles.
2. Haga clic con el botón secundario en Analista de nivel 2 y seleccione Editar en el menú contextual.
3. En la ficha Acceso a la función, haga clic en Editar en Lista
4. Seleccione Referencia de incidente/problema/solicitud
5. Seleccione Modificar en el Nivel de acceso.
El nivel de acceso se actualiza para modificar.
6. Haga clic en Guardar y cierre sesión.
Un mensaje confirma el cambio.
7. Inicie sesión con rol de analista de nivel 2.
8. Seleccione Buscar, Incidentes.

9. Haga clic en Buscar y abra un incidente.

La página Detalles de incidente contiene un botón Editar en lista. Como analista de nivel 2, puede modificar el ticket.

Particiones de datos

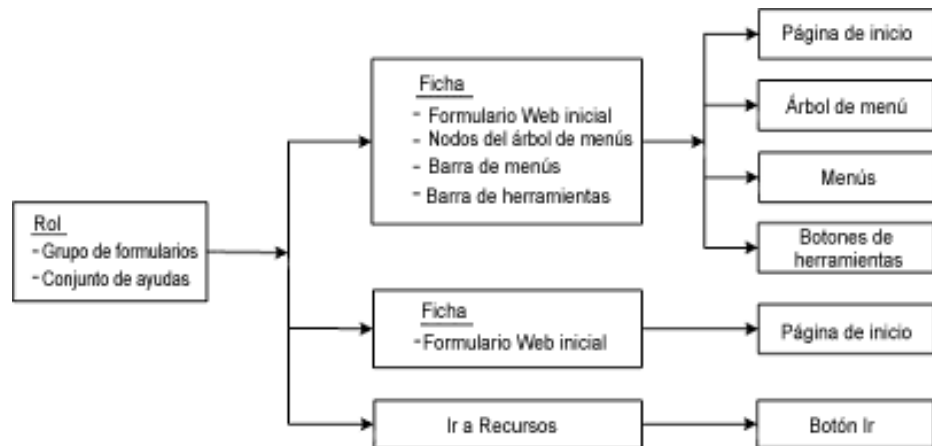
Las particiones de datos son subconjuntos de la base de datos de CA Service Desk Manager que permiten controlar el acceso al nivel de registro. Puede asociar una partición de datos a un rol para controlar el acceso a tickets y otros registros a los que se puede acceder a través de la interfaz Web.

Para obtener información sobre cómo trabajar con las particiones de datos, consulte el tema Asociaciones de particiones de datos (see page 187).

Navegación basada en roles

La vista de la interfaz Web que posee cada usuario está definida por un rol. Los usuarios que cuentan con varias asignaciones de roles pueden elegir entre varias vistas de la interfaz Web.

El siguiente diagrama muestra cómo se relacionan los roles con otros objetos para generar una presentación basada en roles de la interfaz de usuario.



Fichas

Una ficha es una entidad de visualización gráfica que se vincula con un rol para presentar funciones a los usuarios de ese rol. Cuando un usuario se conecta al sistema, la ventana principal muestra las fichas asignadas al rol predeterminado del usuario.

Las fichas definen subdivisiones principales en la ventana principal de la interfaz Web. Cada ficha está configurada para mostrar un conjunto de funciones de la interfaz de usuario adecuado para el rol o roles que la usan.

Todos los roles deben tener por lo menos una ficha. Se pueden asociar una o varias fichas a un rol. Cada ficha tiene un número de secuencia que controla su orden de visualización en la ventana principal. Si solamente se asocia una ficha a un rol, aparecerá la página de inicio de la ficha, no la ficha.

Puede configurar las fichas para incluir las siguientes clases de funciones de visualización:

- Una página de inicio (formulario Web predeterminado) que aparece cuando un usuario selecciona la ficha. La página de inicio es un elemento obligatorio de todas las fichas. Sólo se puede asignar una página de inicio a cada ficha.

Nota: Puede configurar una página de inicio de modo que muestre informes gráficos de objeto de negocio, lo que permite a los usuarios generar informes en tiempo de ejecución. Para obtener más información, consulte el tema Informes de CA Business Intelligence (see page 709).

- Una barra de menús, que presenta listas desplegables de comandos, como los comandos Archivo, Ver y Buscar. La barra de menús es opcional. Sólo se puede asignar una barra de menús a cada ficha.
- Una barra de herramientas, que presenta botones de herramientas para acceder fácilmente a los comandos del menú utilizados con frecuencia. La barra de herramientas es opcional.

CA Service Desk Manager proporciona varias fichas predefinidas. Puede asignar las fichas predefinidas a un rol, modificar las fichas predefinidas y crear fichas personalizadas.

Importante: no asigne más fichas de las que la ventana del explorador puede mostrar; si lo hace, las fichas con números de secuencia más altos se extenderán más allá del área visible de la ventana y el usuario no podrá acceder a ellas.

Importante: incluya sólo fichas que contengan formularios que estén incluidos en el grupo de formularios asignado al rol que vaya a crear o editar. Por ejemplo, no asigne la ficha Cliente ni Empleado al rol Administrador; si lo hace, se generará un error cuando los usuarios intenten acceder a esa ficha. El grupo de formularios del rol se especifica en el campo Grupo de formularios de personalización de la página Detalles del rol. También aparece en la columna Grupo de formularios de la página Lista de roles. Para obtener una lista de los formularios Web de cada grupo de formularios, consulte el tema Grupos de formularios (see page 1059).

Fichas predefinidas

La tabla siguiente muestra las fichas predefinidas asignadas a cada rol. Las fichas se clasifican en orden de número de secuencia, indicando su posición de izquierda a derecha en la ventana.

Nota: En muchos casos, hay versiones múltiples de fichas con el mismo nombre para mostrar. Por ejemplo, la ficha Service Desk del rol Administrador ofrece acceso total a la funcionalidad de CA Service Desk Manager, mientras que la ficha Service Desk del rol Gestor de cambios se centra más en las órdenes de cambio.

Función	Fichas
Administrador	■ Ficha Service Desk con panel de resultados y menú completos ■ ficha Conocimientos ■ Ficha Administración con árbol de menú completo ■ Ficha Informes: administrador ■ Ficha Calendario de cambios ■ Ficha CA CMDB ■ Ficha Automatización de soporte
Gestor de cambios	■ Ficha Informes: gestor de cambios ■ Ficha Service Desk: gestor de cambios ■ Ficha Calendario de cambios
Administrador de configuración	■ Ficha CA CMDB ■ Ficha Administración: administrador de configuración
Analista de configuración	■ Panel de resultados de CA CMDB: analista de configuración
Visor de configuración	■ Panel de resultados de CA CMDB: visor de configuración
Cliente	■ Ficha Cliente
Gestor de servicio al cliente	■ Ficha Service Desk - Gestor de servicio al cliente ■ ficha Conocimientos ■ Ficha Informes - Gestor de servicio al cliente
Representante del servicio de atención al cliente	■ Ficha Service Desk: representante del servicio al cliente ■ Ficha Perfil rápido ■ ficha Conocimientos
Empleado	■ Ficha Empleado

Función	Fichas
Gestor de incidentes	■ Ficha Informes: gestor de incidentes ■ Ficha Service Desk: gestor de incidentes ■ ficha Conocimientos
Analista de conocimiento	■ Ficha Service Desk: analista de conocimiento ■ ficha Conocimientos ■ Programación de la gestión del conocimiento ■ Ficha Tarjeta de informes de conocimiento ■ Ficha Informes: analista de conocimiento
Gestor de conocimientos	■ Ficha Service Desk: gestor de conocimiento ■ ficha Conocimientos ■ Programación de la gestión del conocimiento ■ Ficha Administración: gestor de conocimiento ■ Ficha Tarjeta de informes de conocimiento ■ Ficha Informes: gestor de conocimiento
Administrador de gestión del conocimiento	■ Ficha Administración: administrador de conocimiento
Analista de nivel 1	■ Ficha Service Desk: analista de nivel 1 ■ Ficha Perfil rápido ■ ficha Conocimientos
Analista de nivel 2	■ Ficha Service Desk: analista de nivel 2 ■ ficha Conocimientos ■ Ficha Calendario de cambios
Gestor de problemas	■ Ficha Informes. gestor de problemas ■ Ficha Service Desk: gestor de problemas ■ ficha Conocimientos
Administrador de Service Desk	■ Ficha Administración: administrador de Service Desk
Service Desk Manager	■ Ficha Informes: gestor de Service Desk ■ Ficha Service Desk: gestor de Service Desk ■ ficha Conocimientos ■ Ficha Calendario de cambios
Administrador de Automatización de soporte	■ Ficha Service Desk: analista de nivel 1 ■ Ficha Automatización de soporte

Función	Fichas
	■ Administrador de Automatización de soporte ■ Ficha Perfil rápido ■ ficha Conocimientos
Analista de Automatización de soporte	■ Ficha Service Desk: analista de nivel 1 ■ Ficha Automatización de soporte ■ Ficha Perfil rápido ■ ficha Conocimientos
Administrador del sistema	■ Ficha Administración: administrador del sistema
Administrador de clientes	■ Ficha Administración: administrador de clientes
Analista de distribuidores	■ Ficha Service Desk: Analista de distribuidores

Formularios Web

Los formularios Web definen las páginas que aparecen en la interfaz Web de CA Service Desk Manager.

Hay cuatro tipos de formulario Web:

- URL de informe de objetos de negocio
- Página HTML
- Recurso de IR
- Personalizado (por ejemplo, una URL para una página Web de terceros)

Para obtener información sobre cómo crear formularios Web personalizados, consulte Creación de registros de formularios Web (see page 260).

Grupos de formularios

Los grupos de formularios definen los conjuntos de páginas de la interfaz Web de CA Service Desk Manager de los que dispondrá un rol. Cada rol tiene un grupo de formularios. Los usuarios pueden mostrar sólo las páginas Web incluidas en el grupo de formularios asignado a su rol.

Cada tipo de interfaz tiene un grupo de formularios asociado, un conjunto de archivos HTML que definen las páginas que los usuarios con ese tipo de interfaz pueden ver.

CA Service Desk Manager proporciona los siguientes grupos de formularios predefinidos:

- Analista
- Cliente
- Empleado
- ITIL

Puede utilizar los grupos de formularios predefinidos con su configuración predeterminada, modificar los grupos de formularios predefinidos y crear nuevos grupos de formulario usando Web Screen Painter. Puede ver un listado de los nombres de archivos HTML incluidos en cada grupo de formularios (see page 1059) predefinido.

Árboles de menús

Los árboles de menús son las listas jerárquicas de nodos (recursos de árbol de menús) que aparecen en el panel de navegación situado a la izquierda de la ventana principal de la interfaz Web.

Un rol puede tener un árbol de menús, que proporciona nodos para el acceso a muchas áreas funcionales del sistema. Por ejemplo, el rol de administrador predefinido tiene un árbol de menús que incluye nodos a las opciones de administración de Gestión de sistema y rol, las opciones de administración del Centro de servicio al usuario y muchos otros.

En los roles que incluyen un árbol de menús, éste ofrece acceso a un conjunto especificado de recursos para acceder a áreas funcionales del sistema.

CA Service Desk Manager proporciona árboles de menús predefinidos para los siguientes roles:

- Administrador (admin_tree)
- Administrador de CA CMDB (cmdb_adm_tree)
- Administrador de gestión del conocimiento (kt_adm_tree)
- Gestor de conocimientos (kt_mgr_tree)
- Administrador de Automatización de soporte (sa_admin_tree)
- Administrador de Service Desk (sd_adm_tree)
- Administrador del sistema (sys_adm_tree)
- Administrador de clientes (tn_admin_tree)

Puede editar los campos Nombre, Estado del registro y Descripción de los registros de árboles de menús predefinidos, pero no puede personalizarlos agregando ni eliminando sus recursos de árbol de menús.

Para generar un árbol de menús personalizado, puede crear un nuevo registro de árbol de menús o copiar uno de los árboles de menús predefinidos y personalizarlo.

Nota: El campo Interno (que no se puede modificar) de cada registro de árbol de menús indica si se puede personalizar el árbol de menús. Si el valor del campo Interno es SÍ, indica un árbol de menú predefinido, que no se puede personalizar. Si el valor es NO, indica un árbol de menú definido por el sitio, que se puede personalizar. El botón Personalizar menú sólo aparece en registros de detalles de árbol de menús cuyo valor en el campo Interno sea NO.

Cuando se adjunta un árbol de menús a una ficha, éste pasa a estar disponible para todos los roles que tienen acceso a dicha ficha.

Recursos de los árboles de menús

Los recursos de los árboles de menús definen los elementos a los que pueden acceder los usuarios desde el árbol de menús.

Un recurso de árbol de menús consta de un nombre, su descripción y un fragmento de URL o nombre de archivo HTML utilizado por el motor Web que controla la página Web mostrada.

Barras de menús

Una barra de menús es un elemento de la interfaz de usuario que muestra una lista horizontal de menús en la ventana principal de la interfaz Web. Cada menú contiene una lista desplegable de opciones o comandos. Puede definir barras de menús personalizadas para cualquiera de los roles personalizados que pueda crear.

Los registros de la barra de menús especifican el formulario HTML que controla los elementos de menú a los que puede acceder dicha barra.

Nota: Para definir la funcionalidad de la barra de menús, debe usar la aplicación Web Screen Painter. Para obtener información sobre cómo configurar las funciones de una barra de menús personalizada o predefinida, consulte la *Ayuda en línea de Web Screen Painter*.

La tabla siguiente lista las barras de menú predefinidas e identifica las fichas predefinidas que las utilizan.

Barra de menús	Fichas asociadas
Administración	■ Ficha Administración: administrador de configuración ■ Ficha Administración: administrador de conocimiento ■ Ficha Administración: gestor de conocimiento ■ Ficha Administración: administrador de Service Desk ■ Ficha Administración: administrador del sistema ■ Ficha Administración: administrador de clientes ■ Ficha Administración con árbol de menú completo
CA CMDB	■ Ficha CA CMDB con panel de resultados y menú completos
Calendario de cambios	■ Ficha Calendario de cambios
Conocimientos	■ ficha Conocimientos ■ Programación de la gestión del conocimiento
Service Desk	■ Ficha Service Desk con panel de resultados y menú completos
Service Desk: gestor de cambios	■ Ficha Service Desk: gestor de cambios
Service Desk: gestor de servicio al cliente	■ Ficha Service Desk - Gestor de servicio al cliente
Service Desk: rep. del servicio de atención al cliente	■ Ficha Service Desk: representante del servicio al cliente
Service Desk: gestor de incidentes	■ Ficha Service Desk: gestor de incidentes
Service Desk: analista de conocimiento	■ Ficha Service Desk: analista de conocimiento
Service Desk: gestor de conocimientos	■ Ficha Service Desk: gestor de conocimiento
Service Desk: analista de nivel 1	■ Ficha Service Desk: analista de nivel 1
Service Desk: analista de nivel 2	■ Ficha Service Desk: analista de nivel 2
Service Desk: gestor de problemas	■ Ficha Service Desk: gestor de problemas
Service Desk: gestor del Centro de servicio al usuario	■ Ficha Service Desk: gestor de Service Desk
Service Desk: Analista de distribuidores	■ Ficha Service Desk: Analista de distribuidores
Automatización de soporte:	■ Ficha Automatización de soporte: analista de Automatización

Barra de menús	Fichas asociadas
analista	de soporte

Barras de herramientas

Las barras de herramientas extienden la funcionalidad de las barras de menú agregando la capacidad de mostrar uno o más botones de herramienta a la derecha de los menús.

Los botones de herramienta aparecen como iconos sobre la barra de herramientas. Si hace clic en un botón de herramienta, le da acceso fácil al usuario a comandos u opciones de menú frecuentemente utilizados.

Nota: Utilice la aplicación Web Screen Painter para definir las funciones de la barra de herramientas. Para obtener información sobre cómo configurar las funciones de una barra de herramientas personalizada o predefinida, consulte la *Ayuda en línea de Web Screen Painter*.

Ir a Recursos

El botón *Ir* proporciona un medio sencillo de localizar un registro particular.

Los recursos de *Ir* son un tipo de formulario Web. Si se ha asociado un rol con un recurso de *Ir*, cuando un usuario se conecta con ese rol aparece el botón *Ir* en la esquina superior derecha de la ventana principal de CA Service Desk Manager y en todas las ventanas emergentes. El botón *Ir* tiene dos campos asociados en la interfaz de usuario:

- Una lista desplegable para seleccionar el tipo de registro que se buscará (por ejemplo, orden de cambio)
- Un cuadro de texto para introducir un valor que identifique un registro concreto (por ejemplo, 135 para localizar la orden de cambio 135)

Al asignar recursos de *Ir* a un rol, puede especificar los tipos de registros que los usuarios con ese rol pueden buscar. Por ejemplo, el rol de administrador predefinido tiene los siguientes recursos de *Ir*:

- Orden de cambios
- Documento por ID
- Incidente
- Incidencia
- Conocimientos
- Problema

- Solicitud
- Usuario por ID
- Usuario por nombre
- Usuario por teléfono

Conjuntos de ayudas

Los conjuntos de ayuda son recopilaciones de temas de la ayuda en línea a disposición de los usuarios, en función de los roles que tengan asignados y de la configuración actual de rol. Si se inicia sesión usando el rol Administrador, por ejemplo, se pueden ver los temas de la ayuda en línea incluidos en el conjunto de ayudas correspondiente a administradores. Si se cambia al rol Empleado, se puede ver el conjunto de ayudas correspondiente a empleados.

Cada rol predefinido tiene un conjunto de ayudas predefinido correspondiente. Se pueden crear conjuntos de ayuda personalizados para cualquier rol personalizado que se pueda definir.

Nota: Para obtener información sobre cómo trabajar con definiciones del conjunto de ayudas, consulte la *Ayuda en línea*.

Cómo implementar un rol personalizado

Para muchos sitios, son suficientes los roles predefinidos. Si bien, pueden darse situaciones en las que se desee crear un rol personalizado y adaptarlo para cumplir las necesidades comerciales específicas del sitio dentro de la organización.

El proceso siguiente esboza las tareas necesarias al implementar un nuevo rol. El ejemplo que se muestra aquí describe cómo se puede implementar un rol para un grupo pequeño de analistas encargados de revisar y autorizar tickets de órdenes de cambio.

Para implementar un rol personalizado, ejecute las tareas descritas en el siguiente ejemplo:

1. Cree un nuevo registro de roles mediante los valores de campo siguientes:

Nombre del rol

Analista de cambios

Código

chg_anal

Grupo de formularios de personalización

Analista

Documento preferido

Incidente

2. Seleccione Analista de Service Desk en el campo Partición de datos de la ficha Autorización.
3. Seleccione Modificar en el campo Órdenes de cambio de la ficha de Acceso a función.
4. Introduzca los siguientes valores en la ficha Interfaz Web:

Tipo de interfaz de usuario para Web

Analista

Vista de la ayuda

Analista de cambios

5. Seleccione las siguientes fichas:
 - Ficha Informes: analista de cambios
 - Ficha Service Desk: analista de cambios
 - Ficha Calendario de cambios
 6. Seleccione los siguientes informes en la ficha Formularios Web de informes:
 - Informe de antigüedad de órdenes de cambio activas por prioridad para estados
 - Órdenes de cambio activas a final de semana
 - Órdenes de cambio por tipos de servicio fallidos para categorías de cambios
 7. Agregue el recurso Orden de cambio en la ficha Ir a Recursos.
 8. Cree un conjunto de ayudas personalizado denominado Analista de cambios que incluya todo el contenido pertinente para el nuevo rol.
- Para obtener más información, consulte Cómo crear y publicar un conjunto de ayudas (see page 264).

9. Cree las siguientes fichas personalizadas usando opciones apropiadas para el nuevo rol:
 - Ficha Informes: analista de cambios
 - Ficha Service Desk: analista de cambios
10. Cree un árbol de menús personalizado que incluya todos los nodos apropiados para el nuevo rol.

Para obtener más información, consulte Cómo implementar un árbol de menús personalizado (see page 256).

Cómo implementar un árbol de menús personalizado

Para muchos sitios, son suficientes los árboles de menús predefinidos. Sin embargo, en ciertas situaciones, es posible que desee personalizar un rol mediante la implementación de un árbol de menús personalizado para ese rol.

En la mayoría de los casos, es más fácil comenzar con una copia de un árbol de menús predefinido y después agregar, eliminar o reorganizar los nodos dentro de la jerarquía. Otra alternativa es crear un árbol de menús y desarrollar una jerarquía de nodos completamente nueva.

Puede utilizar cualquiera de los siguientes métodos para poner el árbol de menús personalizado a disposición de un rol:

- Reemplace el árbol de menús del formulario Web (Página de inicio) por la ficha que muestra el archivo `admin_tree` original.
- Cree un formulario Web y adjunte el nuevo formulario Web con el nuevo árbol de menús a una ficha.

Para implementar un menú personalizado, ejecute las siguientes tareas:

1. Copie uno de los árboles de menús predefinidos.

Nota: Anote el valor que introdujo en el campo Código.
2. Cree un formulario Web con los valores de los siguientes campos:

- **Tipo:** HTML
- **Recurso:**

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=admin_main_role.html  
+KEEP.tree_code=menu_tree_code
```

Nota: Especifique el valor del código del árbol de menús creado en el paso 1 para `menu_tree_code`. El código `admin_main_role.html` utiliza el valor de la variable `KEEP.tree_code` como su árbol de menús.

3. Cree un registro de ficha con los valores de los siguientes campos:

- **Página de inicio:** el formulario Web creado en el paso 2
- **Barra de menús:** administración

Nota: La barra de menús Administración es una barra de menús genérica que muchos roles utilizan; no es específica de un rol.

4. Asigne la ficha creada en el paso 3 al rol que desea que tenga acceso al árbol de menús personalizado.
5. Cierre la sesión de CA Service Desk Manager y vuelva a iniciar sesión.
La ficha Administración aparecerá en el árbol de menús personalizado.

Creación de un registro de rol

Los administradores pueden crear roles personalizados para satisfacer requisitos empresariales específicos del sitio.

Procedimiento para crear roles

1. Seleccione Gestión de roles y seguridad, Gestión de roles, Lista de roles en la ficha Administración.
Aparecerá la página Lista de roles.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nuevo rol.
3. Rellene los siguientes campos:

Nombre del rol

Especifica el nombre que identifica el rol siempre que aparece en la interfaz de usuario.

Código

Especifica el código que identifica el rol ante el sistema.

Nota: Después de guardar el registro, el valor de este campo no puede modificarse.

Estado de registro

Indica si el rol está activo o inactivo.

¿Predeterminado?

Indica si este rol es el predeterminado.

Grupo de formularios de personalización

Especifica un grupo de formularios personalizados o predefinidos.

Documento preferido

Especifica el documento usado por este rol para introducir tickets en el sistema.

Descripción

Describe la finalidad del rol. Esta descripción aparece en la página Lista de roles y puede facilitar la tarea de asignar usuarios a los roles pertinentes.

Haga clic en Guardar.

Se guardará la definición del rol y aparecerá la página Detalles del rol.

Creación de un registro de ficha

Puede crear fichas personalizadas con el fin de que aparezcan en la página principal de la interfaz Web. Cuando se vincula un registro de ficha con un registro de rol, el registro de ficha queda disponible para los usuarios asignados a ese rol.

Procedimiento para crear fichas

1. Seleccione Gestión de roles y seguridad, Gestión de roles, Fichas en la ficha Administración.
Aparecerá la página Lista de ficha.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nueva ficha.
3. Rellene los siguientes campos:

Nombre de la ficha

Especifica el nombre que identifica la ficha dentro de la interfaz de administración. Por ejemplo, el nombre de la ficha aparece en la página Lista de fichas.

Código

Especifica el código que identifica esta ficha ante el sistema.

Nota: Una vez definido, este código no puede modificarse.

Estado de registro

Indica si la ficha está activa o inactiva.

Visualizar nombre

Especifica el nombre que aparece en la presentación gráfica de la ficha en la interfaz de usuario.

Página de inicio

Especifica el formulario Web inicial que aparece en la ventana principal cuando un usuario selecciona esta ficha.

Importante: La página de inicio y la barra de menú deben pertenecer al mismo grupo de formularios. Si se define una ficha con una página de inicio y una barra de menú que pertenecen a grupos de formularios (see page 1059) diferentes se producirá un error cuando los usuarios accedan a la ficha.

Barra de menú

Especifica la barra de menú que aparece en la ventana principal cuando un usuario selecciona esta ficha.

Haga clic en Guardar.

La ficha queda creada.

Creación de un registro de barra de menú

Puede crear barras de menú personalizadas para controlar el acceso a las funciones del sistema de los roles definidos por el usuario.

Procedimiento para crear barras de menú

1. En la ficha Administración, vaya a Gestión de roles y seguridad, Gestión de roles, Barras de menú.

Se muestra la página Lista de barras de menú.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nueva barra de menú.

3. Rellene los siguientes campos:

Nombre de barra de menú

(Obligatorio) Especifica el nombre que identifica la barra de menú. Puede usar este campo para identificar mejor las funciones disponibles en la barra de menú.

Código

(Obligatorio) Especifica el código que identifica esta barra de menú ante el producto. Una vez definido, este código no puede cambiarse.

Estado de registro

Indica si la barra de menú está activa o inactiva.

Nombre HTML

Especifica el nombre del formulario HTML que contiene la definición de la barra de menús. La barra de menús se diseña mediante Web Screen Painter.

Descripción

Describe la barra de menús. Utilice esta descripción para seguir identificando esta barra de menús y los roles que utiliza.

Haga clic en Guardar.

Se guardará la definición de la barra de menús y aparecerá la página Detalles de la barra de menús.

Creación de registros de formularios Web

Los administradores pueden crear sus propios formularios Web personalizados para que sean las páginas de inicio de fichas, informes que aparezcan en fichas, recursos del "botón Ir" u otra URL.

Procedimiento para crear formularios Web

1. En la ficha Administración, vaya a Gestión de roles y seguridad, Gestión de roles, Formularios Web.
Aparecerá la página Lista de formularios Web.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nuevo formulario Web.
3. Rellene los siguientes campos:

Nombre del formulario Web

(Obligatorio) Especifica el nombre que identifica el formulario Web.

Estado de registro

Indica si este formulario está activo o inactivo.

Código

(Obligatorio) Especifica el código que identifica el formulario Web ante el sistema. Una vez definido, este código no puede cambiarse.

Nota: Este campo especifica el web_form_name en la ficha Propiedades correspondiente a un formulario de varios marcos en Web Screen Painter.

Tipo

Especifica uno de los siguientes tipos de formulario Web que se está creando:

- **Página HTML:** muestra una página Web que se usa como página de inicio para una de las fichas personalizadas que cree.
- **Informe:** especifica un informe de CA Service Desk Manager que se muestra en cualquier ficha.
- **Ir a Recurso:** especifica un recurso "Botón Ir".
- **Otros:** accede a cualquier otra página Web externa a través de URL.

Descripción

Describe el formulario Web. Utilice esta descripción para identificar más extensamente el formulario Web, el lugar donde aparecerá y su propósito.

Recurso

Especifica el código que llama al formulario Web. Puede ser un código de línea de comandos o una URL.

Por ejemplo: Abra un formulario html "menu_tab_dflt.html":

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=menu_tab_dflt.html
```

Haga clic en Guardar.

Cómo copiar árboles de menús

Puede copiar un árbol de menús existente para utilizarlo como punto de partida de un árbol de menús personalizado.

Procedimiento para copiar árboles de menús

1. Seleccione Gestión de roles y seguridad, Gestión de roles, Árboles de menús en la ficha Administración.

Aparecerá la página Lista de árboles de menús.

2. Haga clic en el árbol de menús para copiarlo.

Aparecerá la página Detalles del árbol de menús.

3. Haga clic en Archivo, Copiar.

Aparecerá la página Crear nuevo árbol de menús.

4. Rellene los siguientes campos:

Nombre de árbol de menús

(Obligatorio) Especifica el nombre que se asigna para identificar este árbol de menús.

Código

(Obligatorio) Especifica el código que identifica el árbol de menús ante el sistema. Una vez definido, este código no puede cambiarse.

Estado de registro

Indica si el árbol de menús está activo o inactivo.

Descripción

Describe el árbol de menús. Esta descripción se puede usar para proporcionar más detalles acerca del árbol de menús y de los roles que lo usan.

Haga clic en Guardar.

Aparecerá la página Detalles del árbol de menú correspondiente al nuevo árbol de menús.

5. Haga clic en Personalizar menú.

Aparece una copia del árbol de menús original.

6. Personalice el árbol de menús como desee.

Nota: Para obtener detalles sobre cómo agregar, eliminar o editar recursos del árbol de menús, consulte la *Ayuda en Línea*.

Cómo crear y personalizar un árbol de menús

Puede crear y personalizar árboles de menús basado en uno de los árboles de menús predeterminados proporcionados.

Cómo crear y personalizar un árbol de menús

1. Seleccione Gestión de roles y seguridad, Gestión de roles, Árboles de menús en la ficha Administración.

Aparecerá la página Lista de árboles de menús.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nuevo árbol de menús.

3. Rellene los siguientes campos:

Nombre de árbol de menús

(Obligatorio) El nombre que se asigna para identificar este árbol de menús.

Código

(Obligatorio) El código que identifica el árbol de menús ante el sistema. Una vez que se ha definido, este código no puede cambiarse.

Estado de registro

Indica si el árbol de menús está activo o inactivo.

Descripción

Es una descripción del árbol de menús. Esta descripción se puede usar para proporcionar más detalles acerca del árbol de menús y de los roles que lo usan.

4. Haga clic en Guardar.

5. Haga clic en Personalizar menú.

Aparece un formulario que le permite personalizar el árbol de menús. En este momento, el árbol de menús contiene solamente un nodo superior con el texto que introdujo como el nombre del árbol de menús.

6. Haga clic con el botón derecho del ratón en el nodo en el árbol de menús y seleccione Crear nuevo nodo.

Aparecerá la página Crear nuevo nodo.

7. Rellene los siguientes campos:

Nombre de nodo

Introduzca el nombre del nodo. Es el nombre que aparece en el árbol de menús.

Descripción

Introduzca una descripción del nodo. La descripción puede utilizarse para definir más extensamente el propósito del nodo.

Recurso

Introduzca el nombre del recurso directamente en el campo o haga clic en el icono de búsqueda para seleccionar el recurso en una lista. El recurso del árbol de menús determina la acción que debe ejecutarse cuando el usuario selecciona el nodo del árbol de menús.

8. Repita los pasos 6 y 7 tantas veces como necesario para crear el conjunto de nodos que quiere que aparezca en el árbol de menús.

Nota: Para obtener más información sobre cómo agregar, eliminar o editar recursos del árbol de menús, consulte la *Ayuda en Línea*.

9. Haga clic en Guardar.

Se guardará la definición del recurso de árbol de menús y aparecerá la página Detalles del árbol de menús.

Creación y publicación de un conjunto de ayuda

Se pueden crear conjuntos de ayuda personalizados para cualquier rol personalizado que se pueda definir.

Procedimiento para crear, rellenar y publicar un conjunto de ayuda

1. Seleccione Gestión de roles y seguridad, Gestión de roles, Conjuntos de ayudas en la ficha Administración.

Aparecerá la página Lista de configuración de la ayuda.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nuevo conjunto de ayudas.

3. Rellene los siguientes campos:

Nombre del conjunto de ayudas

Es el nombre exclusivo de este conjunto de ayudas.

Tipo de interfaz

Es el tipo de interfaz del conjunto de ayudas (por ejemplo, Analista, Empleado o Cliente).

Estado de registro

Indica si el conjunto de ayudas está activo o inactivo.

Prefijo del nombre de archivo

Es el prefijo que desea adjuntar a los archivos de ayuda generados para este conjunto de ayudas. No incluya espacios en el nombre.

Nota: Asigne un prefijo que le permita identificar los archivos pertenecientes a este conjunto de ayuda. Por ejemplo, tal vez desee utilizar ANAL como prefijo del conjunto de ayudas de analista.

Interno

En los conjuntos de ayuda definidos por el usuario, esta opción se establece automáticamente en NO. El valor de este campo no se puede cambiar.

4. Haga clic en Guardar.

Aparecerá la ficha Contenido.

5. Haga clic en Definición de contenido

Se abrirá la ventana Actualización de ayuda seleccionada.

6. Seleccione el contenido que desee incluir en el conjunto de ayudas.

Importante: Algunos temas son obligatorios y se incluirán en el nuevo conjunto de ayudas aunque no los seleccione. Por ejemplo, la página principal de CA Service Desk Manager y otros temas principales se incluyen siempre. Además, los temas anidados dependen de los temas contenedor. Los temas contenedor se incluirán automáticamente si se incluye cualquiera de sus temas anidados. Por ejemplo, si selecciona el tema "Usar el panel de resultados", se incluirá el tema contenedor "Exploración de CA Service Desk Manager" cuando se publique el conjunto de ayudas.

7. Haga clic en OK.

Se cerrará la ventana Actualización de ayuda seleccionada y aparecerá la lista de contenidos en la ficha Contenido.

8. Haga clic en Publicar.

De este modo, se genera el conjunto de ayudas, empaquetando los temas seleccionados en un sistema de ayuda que puede ver en un explorador Web.

9. Espere unos instantes a que termine el proceso de publicación; después, seleccione Vista, Actualizar en la barra de menús.

Se activa el botón Ver ayuda.

10. Haga clic en Ver ayuda.

El conjunto de ayudas personalizado aparece en el explorador Web predeterminado.

Cambio de roles

Cualquier usuario que tenga múltiples roles asignados puede cambiar de rol sin cerrar sesión y volver al sistema. Los roles se asignan a los usuarios sobre la base de sus registros de contacto o su tipo de acceso.

Nota: Para obtener información, consulte Cómo configurar cuentas de usuario (see page 199).

Procedimiento para cambiar roles

1. Seleccione el rol deseado en la lista desplegable Rol en la esquina superior derecha de la página principal de CA Service Desk Manager.
2. Haga clic en Establecer rol.

La interfaz Web y la funcionalidad disponible para los usuarios conectados cambia para coincidir con el rol actual.

Capítulo 7: Establecimiento de la estructura de soporte - CA

Esta sección contiene los siguientes temas:

- [Estructura de soporte](#) (en la página 267)
- [Modelos](#) (en la página 268)
- [CA Workflow](#) (en la página 271)
- [Integración del workflow de CA IT PAM](#) (en la página 274)
- [Códigos compartidos](#) (en la página 281)
- [Códigos de estado](#) (en la página 284)
- [Tipos de tareas](#) (en la página 289)
- [Seguimiento de incidentes](#) (en la página 290)
- [Área de solicitud/incidente/problema](#) (en la página 292)
- [Orden de cambio y categorías de incidencia](#) (en la página 295)
- [Cierre automático de tickets](#) (en la página 302)
- [Actividades del ticket relacionado](#) (en la página 305)
- [Cálculo de prioridad](#) (en la página 307)
- [Controles de atributo dependiente y transiciones de estado](#) (en la página 323)
- [Transiciones de estado para el autoservicio](#) (en la página 336)
- [Temporizadores](#) (en la página 341)
- [Zonas horarias](#) (en la página 341)
- [Adjuntos de archivos](#) (en la página 344)
- [Anuncios](#) (en la página 349)
- [Configuración de consultas almacenadas](#) (en la página 351)
- [Números de secuencias](#) (en la página 352)
- [Uso de registros de auditoría](#) (en la página 353)
- [Integración con CA Network and Systems Management](#) (en la página 353)

Estructura de soporte

La *estructura de soporte* del centro de servicio al usuario está compuesta por los componentes que necesitan los usuarios para resolver problemas. Puede configurar la estructura de soporte de CA Service Desk Manager para que coincida con su modelo de soporte (interno, externo o ambos).

Nota: Es posible personalizar las incidencias, solicitudes y órdenes de cambio para que se ajusten a las necesidades del sitio. Para obtener más información, consulte la *Guía de implementación* y la *ayuda en línea*.

Modelos

CA Service Desk Manager admite estos modelos de servicio de asistencia:

- Modelo interno
- Modelo externo
- Modelo combinado

Nota: Para obtener información sobre cómo utilizar la interfaz Web para implementar el modelo seleccionado, consulte la *Ayuda en línea*.

Modelo interno

Los servicios de asistencia internos admiten empleados que trabajan para la compañía y que tienen problemas con los productos y los servicios que ésta les proporciona, o bien, desean formular preguntas sobre ellos. En CA Service Desk Manager, las solicitudes constituyen la unidad básica de soporte de los servicios de asistencia internos como se indica a continuación.

- Las solicitudes son tickets que administran las preguntas o los problemas de los empleados, y están orientados al soporte de infraestructuras que pertenecen a la organización de soporte, la cual las administra.
- Las órdenes de cambio son tickets que administran los cambios en la infraestructura empresarial a la que se ofrece soporte. Los servicios de asistencia internos suelen emplear las solicitudes como parte principal, a las que se adjuntan órdenes de cambios en caso de que tengan como consecuencia la aplicación de algún cambio en la infraestructura.

Si dispone de un servicio de asistencia interno, realice las tareas siguientes:

- Revisar los tipos de acceso de los empleados utilizando la función administrativa de la interfaz Web para ver si satisface sus necesidades. Si la mayoría de los contactos son empleados que acuden al servicio en busca de asistencia, conviene definir el acceso de empleado como tipo predeterminado. Así se evita tener que definir el tipo de acceso para cada uno de los contactos de empleado a los que presta su ayuda el servicio de asistencia.
- Revisar los tipos de contacto de los empleados utilizando la función administrativa de la interfaz Web para ver si satisface sus necesidades.
- Garantizar que los contactos estén definidos de manera que dispongan del tipo de acceso y del tipo de contacto apropiados. Por ejemplo, si se define el acceso de empleado como tipo predeterminado, también es necesario definir el acceso de analista como el tipo de los contactos de analista.

Por lo general, el tipo de contacto se asigna de manera automática en función del modo de creación del contacto pero, en algunos casos, es posible que no se defina ningún tipo. Los empleados que acudan al servicio de asistencia en busca de ayuda deben tener el tipo de contacto de empleado, mientras que los empleados que trabajen como analistas del servicio de asistencia, deben tener el tipo de contacto de analista.

Se puede trabajar con contactos mediante la función administrativa de la interfaz Web.

En los servicios de asistencia internos que ofrecen ayuda a los empleados, la estructura de soporte consiste en las solicitudes y las órdenes de cambios que crean aquéllos así como en las funciones auxiliares subyacentes de ambos tipos de parte. En tanto que administrador, debe configurar la estructura de soporte.

Modelo externo

Los servicios de asistencia externos prestan apoyo a los clientes que adquieren productos o servicios de la compañía y que desean formular preguntas sobre los productos o servicios, o bien, tienen problemas con ellos. En CA Service Desk Manager, las incidencias constituyen la unidad básica de asistencia de los centros de servicio al usuario externo. Las incidencias son partes diseñados para gestionar las preguntas o los problemas de los clientes, que están orientados a la ayuda con los productos y los servicios adquiridos por los clientes.

Si se lleva a cabo un centro de servicio al usuario externo, debe realizar las tareas siguientes:

- Revisar los tipos de acceso de los clientes utilizando la función administrativa de la interfaz Web para ver si satisface sus necesidades. Si la mayoría de los contactos son clientes, conviene definir el acceso de cliente como tipo predeterminado.
- Revisar los tipos de contacto de los clientes utilizando la función administrativa de la interfaz Web para ver si satisface sus necesidades.
- Garantizar que los contactos estén definidos de manera que dispongan del tipo de acceso y del tipo de contacto apropiados. Por ejemplo, si se define el acceso de cliente como tipo predeterminado, también es necesario definir el acceso de analista como tipo de los contactos de analista.

Por lo general, el tipo de contacto se asigna de manera automática en función del modo de creación del contacto pero, en algunos casos, es posible que no se defina ningún tipo. Los clientes que acudan al servicio de asistencia en busca de ayuda deben tener el tipo de contacto de cliente, mientras que los analistas que trabajen en el servicio de asistencia, deben tener el tipo de contacto de analista.

Se puede trabajar con contactos mediante la función administrativa de la interfaz Web.

En los servicios de asistencia externos que ofrecen ayuda a los clientes, la estructura de soporte consiste, sobre todo, en las incidencias que crean aquéllos así como en las funciones auxiliares subyacentes de este tipo de parte. El administrador es el encargado de configurar la estructura de soporte sirviéndose de la información incluida en este capítulo. Cada tema establece si la información se aplica a su modelo.

Modelo combinado

Algunas compañías tienen que disponer de ambos modelos de servicio de asistencia: interno y externo. En este caso, puede llevar a cabo cualquiera de las tareas siguientes:

- Separar los modelos de servicio de asistencia interno y externo con instalaciones de Service Desk independientes.
- Configurar CA Service Desk Manager para admitir ambos modelos.

Esta configuración es la adecuada si los analistas de Service Desk cuentan con formación para prestar ayuda tanto a empleados como a clientes, y si la distinción entre asistencia interna y externa no siempre está clara. Por ejemplo, puede haber empleados que adquieran productos de la compañía o clientes con problemas y preguntas relacionados con la infraestructura de la compañía.

En tanto que administrador, debe configurar la estructura de soporte para un servicio de asistencia interno/externo combinado que conste de incidencias, solicitudes y órdenes de cambio, y sus funciones de soporte subyacentes. Si decide utilizar un servicio de asistencia combinado, es decir, interno y externo, realice lo siguiente antes de configurar una estructura:

- Revisar los tipos de acceso de los empleados y de los clientes utilizando la función administrativa de la interfaz Web para ver si satisface sus necesidades. Si la mayoría de los contactos son clientes, conviene definir el acceso de cliente como tipo predeterminado. Si la mayoría de los contactos son empleados que acuden al servicio en busca de asistencia, conviene definir el acceso de empleado como tipo predeterminado.
- Revisar los tipos de contacto de los empleados y de los clientes utilizando la función administrativa de la interfaz Web para ver si satisface sus necesidades.

- Garantizar que los contactos estén definidos de manera que dispongan del tipo de acceso y del tipo de contacto apropiados. Por ejemplo, si se define el acceso de cliente como tipo predeterminado, también es necesario definir el acceso de analista como tipo de los contactos de analista y el acceso de empleado como tipo de los contactos de empleado.

Por lo general, el tipo de contacto se asigna de manera automática en función del modo de creación del contacto pero, en algunos casos, es posible que no se defina ningún tipo.

- Los clientes que acudan al servicio de asistencia en busca de ayuda deben tener el tipo de contacto de cliente.
- Los empleados que acudan al servicio de asistencia en busca de ayuda deben tener el tipo de contacto de empleado.
- Los empleados que trabajan como analistas del servicio de soporte deben tener un tipo de contacto de analista.

Se puede trabajar con contactos mediante la función administrativa de la interfaz Web.

CA Workflow

Una definición de proceso de CA Workflow se puede asociar con cualquier tipo de ticket de CA Service Desk Manager. La definición del proceso que se aplicará a los tickets individuales viene determinada por la categoría de cambios, la categoría de incidencias o el área de solicitud/incidente/problema a la que se ha asignado el ticket.

Si una definición de proceso de CA Workflow se asocia a una categoría o área, cuando un ticket se asigna a esa categoría o área, CA Workflow crea una instancia de proceso a partir de la definición. El progreso de la instancia de proceso se muestra en la ficha Tareas de workflow del ticket.

Puede instalar opcionalmente CA Workflow durante la instalación de CA Service Desk Manager, o puede indicar que CA Service Desk Manager use una instancia diferente de CA Workflow mediante la actualización de varias opciones en el Gestor de opciones, incluyendo:

CAWF_USERNAME

Especifica el usuario de CA EEM que dispone de acceso total (accede a los recursos "IDE" y "Process") a CA Workflow.

CAWF_PASSWORD

Especifica la contraseña de cawf_username.

CAWF_PM_LOCATION

Especifica la ubicación: `http://<servidor>:8080/pm/`

CAWF_PM_URL

Especifica la URL: `http://<servidor>:8080/pm/services/pmService`

CAWF_WL_LOCATION

Especifica la ubicación: `http://<servidor>:8080/wl/`

CAWF_WL_URL

Especifica la URL: `http://<servidor>:8080/wl/services/wlService`

Estas opciones especifican diversos puntos finales de CA Workflow. En la mayoría de los casos, basta con actualizar el servidor y el puerto de manera que coincidan con la ubicación de CA Workflow.

Importante: Al cambiar el servidor de CA Workflow, es posible que queden inoperativos las categorías existentes, las áreas o los tickets vinculados a las definiciones de procesos y las instancias de procesos del servidor anterior.

Workflow en tiempo de ejecución

Al guardar los tickets con una categoría o área vinculada a alguna definición de proceso de CA Workflow, se crea una instancia de la definición. El progreso de las instancias se muestra en la ficha Tareas de workflow del ticket. Dado que CA Workflow puede incluir ramas, sólo se muestran los elementos de trabajo finalizados y pendientes.

En la ficha Tareas de workflow aparecen todos los elementos de trabajo finalizados y pendientes así como el estado de workflow general. Al hacer clic en el vínculo Nombre de actividad, se muestra la aplicación Web de la lista de trabajo de CA Workflow, que se utiliza para finalizar elementos de trabajo individuales.

Los datos de la ficha Workflow se buscan directamente en el servidor de CA Workflow. Si el servidor de CA Workflow no está disponible, aparece un mensaje de error en la ficha.

Selección de definiciones de procesos de workflow

Una definición de proceso de CA Workflow debe tener un atributo de cadena denominado *usd_persid* que vincule con una categoría de incidencias o cambios, o con el área de solicitud/incidente/problema. Dicho atributo debe estar marcado como parámetro de entrada. Cuando CA Service Desk Manager inicia la instancia de CA Workflow, establece *usd_persid* con el identificador único (*persistent_id*) del ticket. Uno de los usos de *usd_persid* consiste en efectuar llamadas a servicios Web desde CA Workflow a CA Service Desk Manager.

Importante: Las categorías de cambios e incidencias sólo pueden usar uno de los dos, el sistema de workflow (clásico) interno de CA Service Desk Manager o la aplicación CA Workflow; pero no ambos. Las áreas de solicitud/incidente/problema pueden utilizar solamente la aplicación de CA Workflow. El sistema de workflow clásico interno no admite tickets de solicitudes, incidentes o problema.

Procedimiento para seleccionar una definición de proceso de CA Workflow

1. Seleccione una categoría de cambio o incidencia. Por ejemplo, para seleccionar una categoría de cambio, seleccione Centro de servicio al usuario, Órdenes de cambio, Categorías en la ficha Administración.
Aparecerá la página Lista de categorías de cambios.
2. Haga clic en el símbolo de la categoría de cambio que quiere editar.
Aparecerá la página Detalles de categoría de cambios.
3. Seleccione la casilla de verificación Usar CA Workflow en la ficha Workflow.

Nota: Si se continúa este procedimiento y se guarda la categoría, se elimina el workflow de estilo de CA Service Desk Manager adjunto a la categoría.

Aparece una página de selección con las listas de las definiciones de proceso de CA Workflow disponibles.

4. Seleccione una definición de proceso de CA Workflow.
La categoría se rellena con la selección.
5. Haga clic en Guardar.
La categoría se actualiza con la definición de proceso seleccionada.
6. (Opcional) Cambie la definición de proceso de CA Workflow vinculada editando la categoría y haciendo clic en el hipervínculo de la definición de CA Workflow.

Aparecerá la página de selección de definiciones de procesos.

Nota: Las definiciones de procesos de CA Workflow sólo figuran en la página de selección si poseen el atributo de cadena `usd_persid`. Cuando se inician las definiciones, se define este atributo en el valor de `persistent_id` del parte oportuno. De manera opcional, las definiciones de procesos de CA Workflow incluyen parámetros de entrada de cadena llamados *label*. Si hay uno de estos parámetros *label* definido, CA Service Desk Manager define su valor como el número de ticket. El número de ticket se muestra en la lista de trabajo de CA Workflow y proporciona contexto para los elementos de trabajo.

Tareas de workflow

Las tareas de workflow identifican las actividades que se deben completar en tickets asociados con una categoría o área específica. Al igual que sucede con las propiedades y con otros aspectos de las categorías o áreas, las tareas se agregan de forma automática a los tickets al seleccionar una categoría. La definición de tareas de workflow permite:

- Especificar y describir el tipo de tarea que se debe ejecutar.
- Asignar números secuenciales a cada tarea.
- Especificar el usuario que debe realizar las tareas.
- Realizar un seguimiento del progreso para la resolución de las tareas asignando estados específicos válidos para cada tarea.

Cuando cambia el estado de una tarea se pueden ejecutar ciertos comportamientos. Los comportamientos permiten definir las tareas o procesos específicos que se efectúan cuando las tareas de workflow alcanzan los estados pertinentes. Un comportamiento puede consistir, por ejemplo, en enviar por correo electrónico una notificación a un gestor concreto cuando una tarea de aprobación entre en el estado Pendiente.

Nota: Para obtener más información acerca de cómo crear tareas de workflow y definir sus comportamientos, consulte la *Ayuda en línea*.

Integración del workflow de CA IT PAM

CA IT PAM es un producto independiente de CA con características para automatizar y seguir tareas de administración de hardware y software en entornos de TI de empresa. CA IT PAM automatiza tareas y gestiona interacciones de usuarios, como aprobaciones y notificaciones de conformidad y precisión dentro de los entornos de producción.

Cuando integra CA Service Desk Manager y CA IT PAM, puede sacar provecho de los beneficios de las capacidades de workflow de CA IT PAM desde puntos clave dentro de CA Service Desk Manager. Una integración efectiva entre CA Service Desk Manager y CA IT PAM exige que entienda los dos productos.

Más información:

[Componentes de CA IT PAM](#) (en la página 275)
[Integración de CA IT PAM con CA Service Desk Manager en tiempo de ejecución](#) (en la página 276)
[Cómo crear una definición de proceso](#) (en la página 277)
[Creación de formularios de solicitud de inicio](#) (en la página 278)
[Adjuntar una definición de proceso de CA IT PAM](#) (en la página 280)

Componentes de CA IT PAM

CA IT PAM ofrece varias características y estructuras que facilitan una amplia gama de actividades como parte de la gestión de procesos de CA IT PAM. Sin embargo, en el caso de la integración con CA Service Desk Manager, solamente los siguientes componentes de CA IT PAM son críticos para la integración de CA IT PAM:

- **Definición de proceso:** identifica una serie colectiva de tareas, pasos y condiciones que se estructuran en un orden específico para que diversos individuos o partes puedan iniciarlos y completarlos. Este componente es el pilar de todo el contenido de CA IT PAM.
- **Formulario de solicitud de inicio:** objeto que contiene información descriptiva para los usuarios finales. El formulario de solicitud de inicio presenta a los usuarios una definición de proceso mientras se ocultan los detalles técnicos de la misma.
- **Palabras clave:** lista de frases o palabras clave predefinidas para adjuntar a los formularios de solicitud de inicio.
- **Biblioteca de automatización:** área de CA IT PAM que almacena y muestra definiciones de proceso y formularios de solicitud de inicio.
- **Ruta de la biblioteca o ruta de referencia:** estructura de carpeta que organiza y describe definiciones de proceso y formularios de solicitud de inicio en la biblioteca de automatización.
- **Instancia de proceso:** entidad activa que ejecuta las reglas que se definen en una definición de proceso. La instancia de proceso progresa hasta que se completa el estado de definición de proceso.
- **Mensajes de registro de la instancia de proceso:** registro configurable y en ejecución que detalla la evolución de las actividades de la instancia de proceso. Las categorías de mensaje de registro son útiles para la integración de CA Service Desk Manager con CA IT PAM.

Nota: El alcance de las definiciones de los componentes de CA IT PAM se limita a su uso en CA Service Desk Manager. Para obtener información sobre características y componentes de CA IT PAM, consulte la documentación de CA IT PAM.

Integración de CA IT PAM con CA Service Desk Manager en tiempo de ejecución

Cuando habilita la integración, los usuarios de CA Service Desk Manager experimentan lo siguiente:

- En una nueva petición, orden de cambio o incidencia, una instancia de proceso de CA IT PAM se inicia basado en la categoría o el área del ticket. La información resumida inmediatamente aparece en la ficha Tareas de workflow.
- Cuando un área de petición, categoría de cambio o categoría de incidencia cambia, se termina una instancia de proceso de CA IT PAM adjunta y se inicia una nueva instancia de proceso.
- Cuando un usuario de CA Service Desk Manager intenta cerrar una petición, orden de cambio o incidencia donde la instancia de proceso de CA IT PAM no esta completa todavía, el usuario no puede cerrar el ticket. En su lugar, el usuario debe cancelar primero el ticket. El estado de cancelación termina la instancia de proceso de CA IT PAM antes de que el ticket se cierre.
- Cuando un usuario desea entender el estado de la instancia de proceso sin salir del ticket, puede hacer clic en la ficha Tareas de workflow del ticket. La ficha Tareas de workflow muestra la fecha de inicio, la fecha de finalización y el estado actual de la instancia de proceso, así como una pista de auditoría actual de mensajes que indican la ruta de la instancia de proceso.
- Cuando un usuario desea ver la ruta actual de la instancia de proceso en relación con todo el proceso, puede seleccionar el botón Ver proceso de la ficha Tareas de workflow. El botón Ver proceso inicia una instantánea gráfica de toda la instancia de proceso y muestra la ruta actual.
- Cuando un usuario desea ver los formularios de solicitud de interacción de CA IT PAM que están esperando una acción por parte del usuario, puede seleccionar cualquier entrada en la ficha Tareas de workflow. La ficha Tareas de workflow contiene una pista de auditoría de los mensajes de instancia de proceso que aparecen en la lista de tareas de CA IT PAM.

Nota: Cuando un usuario selecciona el botón Ver proceso de CA Service Desk Manager o los mensajes de instancia de proceso de CA IT PAM, el sistema solicita un nombre de usuario y una contraseña de CA IT PAM para una sola sesión de explorador. Después de la solicitud inicial, el sistema no vuelve a solicitar esta información al usuario hasta que se cierra el explorador de CA Service Desk Manager.

Cómo crear una definición de proceso

Cuando cree la definición de proceso, rellene CA IT PAM con contenido que vaya a aparecer en CA Service Desk Manager. Utilice al diseñador de procesos gráficos de CA IT PAM para crear, probar e introducir una definición de proceso. En CA Service Desk Manager, también puede crear macros para iniciar procesos de CA IT PAM.

Nota: Para obtener información sobre cómo crear macros de CA IT PAM, consulte la *Ayuda en línea*.

Para crear una definición de proceso en CA IT PAM, realice lo siguiente:

1. Inicie sesión en el cliente de CA IT PAM como usuario administrativo.
2. Utilice al diseñador de procesos gráficos de CA IT PAM para crear, probar e introducir una definición de proceso. Cuando trabaje con la definición de proceso, utilice las instrucciones en la documentación de usuario de CA IT PAM.

Nota: Si se produce un fallo al introducir la definición de proceso antes de intentar utilizarla, el workflow no puede funcionar correctamente en CA Service Desk Manager.

Los elementos de definición de proceso siguientes están disponibles en CA Service Desk Manager:

Nombre de proceso

Aparece en la páginas Área de petición, Categoría de cambio y Detalles de incidencia. El nombre del proceso también aparece en la ficha Tareas de workflow de un ticket. El nombre del proceso describe la definición de proceso a CA Service Desk Manager a analistas y a otros usuarios que gestionan tickets.

Ruta de referencia de proceso

Aparece en las páginas Área de petición, Categoría de cambio y Detalles de Incidencia. La ruta de referencia de proceso también aparece en la ficha Tareas de workflow del ticket. La ruta de referencia de proceso puede ser útil para describir el propósito del proceso a usuarios finales. Por ejemplo, "/Processes/Approval" no es útil. En cambio, una ruta de referencia como "/Office Supplies/Approvals/Over-200-USD" describe el flujo de trabajo para gestionar órdenes que superan los \$200 dólares estadounidenses.

Mensajes del registro de procesos

Aparece en la ficha Tareas de workflow del ticket de CA Service Desk Manager. De manera predeterminado, un registro de actividades se almacena con la instancia de proceso. Los mensajes del registro de procesos tienen la categoría Proceso. Un diseñador de procesos puede crear mensajes personalizados para que aparezcan en la ficha Tareas de workflow de un ticket de CA Service Desk Manager.

Nota: Para obtener información sobre cómo configurar la opción `caextwf_log_categories` para gestionar mensajes de registro, consulte la *Guía de implementación*.

Creación de formularios de solicitud de inicio

Cuando cree un formulario de petición de inicio, asócielo con la definición de proceso e introdúzcalo. Incluya las palabras clave apropiadas en las propiedades del formulario de petición de inicio. Si falta la palabra clave apropiada en las propiedades del formulario de petición de inicio, dicho formulario y su definición de proceso asociada presentan un fallo al aparecer en CA Service Desk Manager.

Para crear un formulario de petición de inicio

1. Inicie sesión en el cliente de CA IT PAM como usuario administrativo.
2. Abra la biblioteca de CA IT PAM y desplácese al formulario de petición de inicio de la ruta.

El formulario de petición de inicio aparece en el panel derecho de la biblioteca de CA IT PAM.
3. Seleccione en la lista el formulario de petición de inicio.

Aparecerá un menú contextual.
4. Seleccione Propiedades.

Aparecerá la página Propiedades del objeto de biblioteca.
5. (Opcional) Haga clic en la ficha General y modifique la descripción del formulario de petición de inicio. Agréguele una descripción que identifique el uso correcto del formulario de petición de inicio y la definición del proceso asociada al administrador de CA Service Desk Manager.
6. Haga clic en la ficha Palabras clave.

La ficha Palabras clave está activa.
7. Haga clic en el icono ab+.

Se agrega una fila a la lista vacía.

8. Haga clic en la fila.

Un cursor que parpadea resalta la fila e indica que está preparada para la escritura.

9. Introduzca uno de los valores siguientes para asociar una palabra clave a la categoría o el área de ticket apropiada. Para poner, por ejemplo, un formulario de petición de inicio a disposición para un área de petición de CA Service Desk Manager, introduzca la palabra clave pcat.

Ticket	Usar palabra clave
área de solicitud	pcat
categoría de cambios	chgcats
categoría de incidencias	isscats

10. Agregue una fila a la lista para cada palabra clave aplicable. Para hacer, por ejemplo, que el formulario de petición de inicio aparezca tanto en áreas de petición como en categorías de cambio, agregue una fila para la palabra clave chgcats y otra fila para la palabra clave pcat.

11. Haga clic en OK.

CA IT PAM guarda las palabras clave y la descripción, y cierra el cuadro diálogo Propiedades de objeto de biblioteca.

12. Introduzca el formulario de petición de inicio.

Nota: Si no puede introducir el formulario de petición de inicio, no aparecerá en CA Service Desk Manager.

La información del formulario de petición de inicio de CA IT PAM aparece en la lista de formularios de petición de inicio de CA Service Desk Manager. El administrador de CA Service Desk Manager puede asociar el formulario de petición de inicio de CA Service Desk Manager con la definición de proceso, en un área de petición, categoría de cambio o página Detalles de categoría de incidencia.

Aparecen los siguientes elementos del formulario de petición de inicio en CA Service Desk Manager:

Nombre del formulario de petición de inicio

Aparece en las páginas de lista de categorías de incidencia, categorías de cambio y áreas de solicitud.

Ruta de referencia del formulario de petición de inicio

Aparece en las páginas de lista de categorías de incidencia, categorías de cambio y áreas de solicitud.

Descripción del formulario de petición de inicio

Aparece en las páginas de lista de categorías de incidencia, categorías de cambio y áreas de solicitud. El texto en este campo describe cómo el formulario de petición de inicio es apropiado para la selección en una categoría de incidencia, categoría de cambio o área de petición particular.

Adjuntar una definición de proceso de CA IT PAM

Cuando adjunta una definición de proceso de CA IT PAM a una categoría o área de ticket de CA Service Desk Manager, crea una conexión estática entre una categoría o área de ticket de CA Service Desk Manager y una definición de proceso de CA IT PAM.

Cuando crea un usuario de CA Service Desk Manager o edita un ticket y selecciona una categoría de ticket, se inicia la definición de proceso de CA IT PAM asociada en una instancia de proceso. La información pertinente sobre la instancia de proceso aparece en la ficha Tareas de workflow el ticket.

Para adjuntar una definición de proceso

1. En la ficha Administración, seleccione Service Desk.
2. Desplácese a las categorías o áreas de ticket.

Aparece la lista de áreas o categorías.

3. Cree o edite un área de ticket o categoría.

Aparecerá la página Actualizar.

4. Haga clic en la ficha Workflow.

Si las opciones de CA IT PAM se instalan en el gestor de opciones de CA Service Desk Manager, el botón Utilizar CA IT PAM está disponible en la ficha Workflow.

5. Haga clic en Utilizar CA IT PAM,

Aparece la lista de formularios de petición de inicio de CA IT PAM. Cada fila en la lista es un formulario de petición de inicio de CA IT PAM.

Nota: Puede utilizar CA IT PAM, CA Workflow o el workflow interno de CA Service Desk Manager para gestionar categorías o áreas de ticket diferentes. Sin embargo, una única categoría puede utilizar solamente una herramienta de workflow por vez.

6. Haga clic en el valor en la columna Nombre para seleccionar la definición de proceso asociada con este formulario de petición de inicio.

Se cierra la lista de formularios de petición de inicio de CA IT PAM. El nombre de la definición de proceso y la ruta de referencia de definición de proceso aparecen en la ficha Workflow.

7. Haga clic en Guardar.

El sistema guarda los valores de proceso. El ticket siguiente que un usuario crea en la categoría o el área de ticket especificada automáticamente adjunta el workflow y crea una instancia de proceso. La ficha Tareas de workflow del ticket muestra un resumen de la información de la instancia de proceso. Adicionalmente, un usuario puede acceder a más información sobre la instancia de proceso haciendo clic en Ver proceso en la ficha Tareas de workflow.

Códigos compartidos

En CA Service Desk Manager, los distintos tipos de partes comparten algunos códigos subyacentes como los códigos de prioridad, gravedad, impacto y urgencia. Las solicitudes y las órdenes de cambio comparten algunos códigos, y todos los tipos de tickets comparten otros códigos.

Tenga en cuenta la siguiente información sobre códigos compartidos:

- De forma predeterminada, los valores numéricos los clasifican.
- Los códigos se pueden personalizar.
- Los códigos compartidos no se pueden agregar ni eliminar.
- Puede utilizar códigos de impacto, prioridad, severidad y urgencia.

Según el modelo de servicio de asistencia, configure los siguientes códigos:

Códigos compartidos	Descripción
Prioridad	Se debe configurar para todos los modelos de servicio de asistencia.
Severidad	Se debe configurar para los modelos de servicio de asistencia interno y combinado.
Impacto	Se debe configurar para los modelos de servicio de asistencia interno y combinado.
Urgencia	Se debe configurar para los modelos de servicio de asistencia interno y combinado.

Nota: Para obtener más información acerca de cómo personalizar estos códigos con la función administrativa de la interfaz Web, consulte la *Ayuda en línea*.

Códigos de prioridad

Los códigos de prioridad indican el orden en el que el servicio de asistencia debe responder a los partes, es decir, especifican el grado de atención que deben recibir los partes. Los códigos de prioridad se incluyen en las solicitudes, las órdenes de cambios y las incidencias, por lo que son aplicables a todos los modelos de servicio de asistencia.

Puede utilizar prioridades para escalar tickets manual o automáticamente mediante el control de eventos. En muchas instalaciones de Service Desk, el empleo de códigos de prioridad en el panel de resultados permite informar a los analistas sobre el estado en tiempo real de sus solicitudes y órdenes de cambios.

Existe la opción de asignar tipos de servicios a los códigos de prioridad, que se asignan automáticamente a los partes si se especifica el código de prioridad oportuno. Esto permite asociar un nivel de servicio específico a los partes según la prioridad asignada. Por ejemplo, el tipo de servicio definido por el sistema, resolución de 4 horas, se asocia automáticamente a la prioridad 1. A los tickets que se les asigna una prioridad 1, por lo tanto, se les asigna automáticamente este tipo de servicio, incluyendo todos los eventos de tipo de servicio que están asociados con el tipo de servicio de resolución de 4 horas.

Más información:

[Acuerdos de nivel de servicio](#) (en la página 157)

[Cómo implementar los tipos de servicio](#) (en la página 159)

Códigos de gravedad

Los códigos de gravedad identifican la magnitud de los daños en los equipos a los que afectan las solicitudes. Los códigos de gravedad sólo se incluyen en las solicitudes, por lo que se aplican en exclusiva a los modelos de servicio de asistencia interno y combinado.

Nota: A menudo, se entiende la gravedad como sinónimo de prioridad. Algunos sitios sólo utilizan la prioridad, ignorando por completo la severidad. Si desea diferencia entre la gravedad de un problema desde el punto de vista técnico (severidad) y la rapidez con la que desea administrarlo (prioridad), puede utilizar los códigos de gravedad y de prioridad.

Si el sistema está configurado para utilizar la metodología ITIL, también aparece un campo denominado Valor para cada código de impacto. Este campo ayuda a calcular la prioridad del incidente.

Códigos de impacto

Los códigos de impacto miden la importancia de los partes en cuanto al funcionamiento del sistema. Por ejemplo, si una orden de cambio afecta en teoría al funcionamiento de todo el sistema, se le asigna un impacto alto. Los códigos de impacto sólo se incluyen en las solicitudes y las órdenes de cambios, por lo que se aplican en exclusiva a los modelos de servicio de asistencia interno y combinado.

Nota: Aunque los códigos de impacto y los códigos de urgencia (see page 283) son similares, sus objetivos son distintos.

Códigos de urgencia

Los códigos de urgencia miden la importancia de las solicitudes para los usuarios del sistema, es decir, indican la relevancia de las solicitudes en el entorno de producción general. Por ejemplo, si una solicitud podría arriesgar la misión de la empresa, el código de urgencia puede ser un valor de 5 Inmediatamente. Los códigos de urgencia sólo se incluyen en las solicitudes, por lo que se aplican en exclusiva a los modelos de servicio de asistencia interno y combinado.

Aunque los códigos de urgencia y de impacto tienen objetivos distintos, se confunden con frecuencia dado que sus valores pueden coincidir. Por ejemplo, una solicitud de informar un fuego en un centro de datos importante puede tener un impacto de 3-Un sólo grupo y de urgencia 5-Inmediatamente. Estos códigos se aplican porque el fuego impacta en más de un grupo, pero no necesariamente en toda la organización. Porque el centro de datos es importante para las operaciones, la urgencia requiere atención inmediata.

Códigos de estado

Los códigos de estado se utilizan para realizar el seguimiento del estado de los elementos. Los códigos de estado independientes llevan el seguimiento de solicitudes, órdenes de cambio, incidencias y tareas de workflow. En todos los casos existen códigos de estado predefinidos que se pueden utilizar si satisfacen las necesidades. De no ser así, es posible modificar estos códigos predefinidos o definir otros nuevos específicos del departamento. Según el modelo de servicio de asistencia, es preciso configurar los siguientes códigos:

Códigos de estado	Descripción
Solicitud	Se debe configurar para los modelos de servicio de asistencia interno y combinado.
Orden de cambios	Se debe configurar para los modelos de servicio de asistencia interno y combinado.
Incidencia	Se debe configurar para los modelos de servicio de asistencia externo y combinado.
Tarea	Se debe configurar para todos los modelos de servicio de asistencia.

Los códigos de estado permiten a los analistas ordenar y seleccionar la información basándose en el estado para poder realizar un seguimiento meticuloso de su progreso. La precisión con la que se definan los códigos de estado determina la exactitud con la que los analistas describen el estado real de los elementos.

Los códigos de estado se pueden marcar como activos o inactivos. Al marcarlos como inactivos, dejan de estar a disposición de los analistas para el uso inmediato pero no para su futuro uso, es decir, no se eliminan de las bases de datos. Si, más adelante, conviene emplear los códigos de estado, basta con acceder a ellos y marcarlos como activos.

Nota: Las mismas definiciones de área están disponibles para los tickets de solicitud, incidente y problema. En la ficha Administración, se hace referencia a los tickets como áreas de solicitud/incidente/problema. Para abreviar, aquí se denominan simplemente áreas de solicitud.

Códigos de estado de solicitud

La tabla siguiente describe los códigos de estado predefinidos para los tickets de solicitud.

Código de estado de solicitud	Descripción
Acknowledged (Confirmado)	Se ha confirmado la recepción de la solicitud.
Closed (Cerrado)	Se ha resuelto por completo la solicitud.
Cerrado-sin resolver	Se ha cerrado la solicitud pero aún se tiene que resolver.
Reparación en curso	La solicitud sigue pendiente de reparación.
Hold (En espera)	Los eventos del tipo de servicio de la solicitud permanecen en espera.
Open (Abierto)	Una solicitud ha sido definida y se utiliza para supervisar y gestionar su finalización.
Problema cerrado	Se ha cerrado por completo la solicitud por problema.
Problema reparado	Se ha reparado el problema de la solicitud pero ésta no se ha cerrado.
Problema abierto	Se ha identificado la solicitud como un problema.
Researching (Investigando)	La solicitud permanece abierta con la investigación y el análisis pendientes de finalización.
Trabajo en curso	Se está trabajando para solucionar una solicitud.

En caso de que el sitio use otra terminología para identificar el estado de las solicitudes, se deben definir códigos de estado apropiados y desechar los códigos predefinidos o modificar sus definiciones según los términos empleados. Por ejemplo, tal vez quiera definir códigos de estado de solicitud adicionales, como los siguientes:

Código de estado de solicitud	Descripción
Duplicado	Se ha abierto la solicitud pero quizá sea el duplicado de otra solicitud existente de otro usuario.
Emergency	Solicitudes críticas que se deben atender de inmediato.
Informe	La solicitud está resuelta y cerrada pero se debe elaborar un informe de gestión sobre ella.

Código de estado de solicitud	Descripción
Prueba	La solicitud está resuelta pero se debe poner a prueba durante una semana antes de cerrarla.

Códigos de estado de orden de cambios

La tabla siguiente describe los códigos de estado predefinidos para los tickets de orden de cambio.

Cambio del estado de orden de cambio	Descripción
Aprobación en curso	La orden de cambios permanece abierta pendiente de aprobación.
Aprobado	Se ha aprobado la orden de cambio.
Cancelada	Se ha cancelado la orden de cambios.
Closed (Cerrado)	Se ha finalizado la orden de cambios.
Hold (En espera)	Los eventos del tipo de servicio de la orden de cambios permanecen en espera.
Implementación en curso	Se está implementando la orden de cambios.
Open (Abierto)	Se ha definido la orden como orden de cambios, la cual se emplea para supervisar y gestionar su finalización.
Rechazado	Se ha rechazado la orden de cambio.
Resuelto	Se ha resuelto la orden de cambio.
RFC	Se ha enviado una solicitud de cambio.
Suspendido	Se han detenido las tareas de workflow de la orden de cambios.
Verificación en curso	Se está verificando la orden de cambios.
Revertido	Se ha revertido la orden de cambio implementada.
Implementado	Se ha implementado el cambio.

En caso de que el departamento use otra terminología para identificar el estado de las órdenes de cambios, se deben definir códigos de estado apropiados y desechar los códigos predefinidos o modificar sus definiciones según los términos empleados. Por ejemplo, se podrían definir otros códigos de estado de orden de cambios como los de la siguiente tabla:

Código de estado de solicitud personalizado	Descripción
Duplicado	Se ha abierto la orden de cambios pero quizá sea el duplicado de otra orden de cambios existente de otro usuario.
Emergency	Órdenes de cambios críticas que se deben atender de inmediato.
Informe	La orden de cambios está finalizada y cerrada pero se debe elaborar un informe de gestión sobre ella.

Códigos de cierre

Utilice códigos de cierre para definir el resultado final de órdenes de cambio. Por ejemplo, correcto o incorrecto. Configure los códigos de cierre manualmente o como parte de la actividad de actualización de estado en una orden de cambio cuando el estado sea cerrado, terminado o resuelto.

Nota: Para obtener más información sobre cómo crear o definir códigos de cierre y para ver más datos sobre las opciones *require_closure_code* y *force_closure_code*, consulte la *Ayuda en línea*.

Códigos de estado de incidencia

La tabla siguiente describe los códigos de estado predefinidos para los tickets de incidencia.

Código de estado de incidencia	Descripción
Aprobación en Progreso	La incidencia permanece abierta pendiente de aprobación.
Cancelada	Se ha cancelado la incidencia.
Closed (Cerrado)	Se ha finalizado la incidencia.
Hold (En espera)	Los eventos del tipo de servicio de la incidencia permanecen en espera.
Implementación en curso	Se está implementando la incidencia.
Open (Abierto)	Se ha definido y abierto la incidencia para supervisarla y gestionarla hasta su resolución.

Código de estado de incidencia	Descripción
Suspendido	Se han detenido las tareas de workflow de la incidencia.
Transacción en curso	Se está realizando una transacción con un cliente relacionada con la incidencia.
Verificación en Progreso	Se está verificando la incidencia.

En caso de que el departamento use otra terminología para identificar el estado de las incidencias, se deben definir códigos de estado apropiados y desechar los códigos predefinidos o modificar sus definiciones según los términos empleados. Por ejemplo, es posible que desee definir otros códigos de estado de incidencia como los siguientes:

Código de estado de incidencia personalizado	Descripción
Duplicado	Se ha abierto la incidencia pero quizá sea el duplicado de otra incidencia existente de otro usuario.
Emergency	Incidencias críticas que se deben atender de inmediato.
Informe	La incidencia está finalizada y cerrada pero se debe elaborar un informe de gestión sobre ella.

Códigos de estado de tarea

Los códigos de estado de tarea describen los posibles estados de las tareas de workflow. Cada una de las tareas del workflow de una incidencia u orden de cambios posee su propio estado, que es independiente del estado del ticket. Las tareas de workflow sirven a los analistas para realizar un seguimiento del tiempo que se tarda en finalizar cada una de las tareas correspondientes a cada ticket.

La tabla siguiente describe los códigos de estado predefinidos para las tareas de workflow.

Código de estado de tarea	Descripción
Aprobar	Se ha aprobado la tarea.
Cancelada	Se ha cancelado la tarea y no es posible realizar más actualizaciones.

Código de estado de tarea	Descripción
Finalizada	Se ha finalizado la tarea.
Pendiente	Se ha iniciado la tarea.
Rechazar	Se ha rechazado la tarea.
Volver a abrir	Se ha vuelto a abrir la-tarea.
Reapertura: espere	Se ha abierto de nuevo una tarea anterior.
Omitir	Se ha omitido la tarea.
Espere	No se ha iniciado la tarea.

En caso de que el departamento use otra terminología para identificar el estado de las tareas de workflow, se deben definir códigos de estado apropiados y desechar los códigos predefinidos o modificar sus definiciones según los términos empleados.

Cabe la posibilidad de asignar a cada código de estado de tarea un tipo de comportamiento, el cual se lleva a cabo cuando las tareas alcanzan ese estado. De este modo, se aporta mucha más información acerca del progreso de la tarea. Además, también se puede usar la función de acumulación para realizar un seguimiento del tiempo y del coste que supone la finalización de los partes.

Tipos de tareas

Los tipos de tareas ayudan a determinar el comportamiento de tareas de workflow concretas y los códigos de estado de las tareas. Con objeto de producir características definidoras para cada tipo de tarea, se identifican los códigos de estado de tarea o los estados específicos que se pueden utilizar.

Puesto que tanto las órdenes de cambio como las incidencias utilizan tareas de workflow, es preciso configurar tipos de tareas para todos los modelos de servicios de asistencia. Los códigos de estado de tarea identifican los comportamientos asociados a cada una de las tareas. Por ejemplo, el tipo de tarea de aprobación se puede configurar de manera que disponga de los estados Aprobar, Rechazar, Pendiente y Esperar. Si este tipo de tarea entra en el estado Pendiente, se puede enviar una notificación a un gestor concreto, un analista, etc.

Los tipos de tareas se pueden marcar como activos o inactivos. Al marcarlos como inactivos, dejan de estar a disposición de los analistas para el uso inmediato pero no para su futuro uso, es decir, no se eliminan de las bases de datos. Si decide utilizar el tipo de tarea más adelante, vuelva a marcarlo como activo.

Nota: En la página Lista de tipos de tareas de la función administrativa de la interfaz Web se muestran los tipos de tareas predefinidos.

Ejemplo: códigos de estado de tarea

La tabla siguiente contiene algunos códigos de estado de ejemplo:

Código de estado de tarea	Descripción
Aprobación	Aprobar o rechazar parte
Tarea final de grupo	Fin de tareas del grupo
Tarea inicial de grupo	Inicio de tareas del grupo
Aprobación de inicio	Aprobación para iniciar el parte

En este ejemplo, los tipos Tarea inicial de grupo y Tarea final de grupo definen un grupo de tareas dentro de las categorías de incidencias o de cambios que se deben finalizar. Las tareas del grupo se pueden ejecutar en cualquier orden. Una vez que el tipo Tarea inicial de grupo se encuentra en estado Pendiente (iniciado), se aplica este mismo estado a todas las demás tareas del grupo.

Nota: Para obtener más información acerca de los tipos de tareas, consulte la *Ayuda en línea*.

Seguimiento de incidentes

El seguimiento de incidentes permite a los analistas seguir un incidente mediante la selección de uno o más indicadores para el mismo. La información especificada por los analistas proporciona a su organización métricas sobre incidentes para informes. Por ejemplo, los analistas pueden indicar que un incidente se asignó incorrectamente. Cuando un porcentaje grande de tickets asignados incorrectamente aparece en un informe, su organización se puede dar cuenta de que es necesario ajustar las asignaciones.

Por ejemplo, los analistas pueden especificar información para ayudar a su organización a realizar lo siguiente:

- Mejorar el cierre y la capacidad de respuesta de SLA en niveles más bajos dentro de la organización de soporte.

- Identificar tickets asignados incorrectamente.
- Indicar que se usó una herramienta de control remoto para resolver el ticket.

Puede instalar la opción `efficiency_tracking` del gestor de opciones, para que los analistas puedan utilizar las opciones de seguimiento que aparecen en la ficha Seguimiento de eficiencia de las páginas de detalles de incidente.

Nota: Para obtener más información sobre el seguimiento de incidentes, consulte la *Ayuda en línea*.

Instalación de seguimiento de incidentes

Puede instalar una opción para permitir a los analistas seguir un incidente estableciendo indicadores particulares para el incidente. La información especificada por los analistas proporciona a su organización métricas sobre incidentes para informes. Después de instalar la opción, los indicadores de seguimiento aparecen en la ficha Seguimiento de eficiencia de las páginas de detalles de incidentes.

Procedimiento para instalar el seguimiento de incidentes

1. En la ficha Administración, vaya a Gestor de opciones, Gestor de solicitudes.
Aparecerá la Lista de opciones.
2. Haga clic en `efficiency_tracking`.
Aparecerá la página Detalles de opciones de `efficiency_tracking` con los valores predeterminados definidos.
3. Haga clic en Editar.
Aparecerá la página Actualización de opciones de `efficiency_tracking` con los valores predeterminados definidos, donde podrá modificar la descripción.
4. Haga clic en Instalar.
Aparecerá la página Detalles de opciones de `efficiency_tracking`.
5. Haga clic en Cerrar ventana.
El seguimiento de incidentes queda instalado; sin embargo, la ficha Seguimiento de eficiencia no aparecerá en las páginas de detalles de incidentes.
6. Reinicie CA Service Desk Manager.
La ficha Seguimiento de eficiencia aparece en las páginas de detalles de incidentes.

Área de solicitud/incidente/problema

Las áreas de solicitud definen las agrupaciones lógicas en las que se pueden organizar los tickets de solicitudes, de incidentes y de problemas. Por ejemplo, se pueden asignar tickets pertenecientes a una aplicación al área Aplicaciones predefinida. Siempre que un analista asigna un ticket a un área de solicitud, toda la información que se haya asociado a esa área de solicitud se introducirá automáticamente en el ticket. Por ejemplo, al indicar un tipo de servicio, se asocia al ticket pertinente y a todos sus eventos de tipo de servicio asociados.

Nota: Las mismas definiciones de área están disponibles para los tickets de solicitud, incidente y problema. En la ficha Administración de interfaz Web de CA Service Desk Manager, se hace referencia a estas áreas como áreas de solicitud/incidente/problema. Para abreviar, aquí se denominan simplemente áreas de solicitud.

Puede establecer el estado de cualquier área de solicitud en activo o inactivo. Cuando establece un área de solicitud en inactiva, los analistas ya no podrán utilizarla, pero no se suprime de la base de datos. Si decide más tarde utilizar el área de solicitud, necesita cambiar solamente el estado de vuelta a activo.

Puede utilizar las áreas de solicitud para hacer lo siguiente:

- Especificar valores predeterminados a los campos de grupo y asignatario de los tickets.
- Asociar de forma automática niveles de servicio a los tickets mediante la asignación de tipos de servicios predeterminados a las áreas de solicitud.
- Asociar una encuesta a un área de solicitud.
- Seleccionar y crear un informe sobre los tickets por área definiendo sus propias áreas de solicitud personalizada. Estudiar en el momento oportuno las tendencias de las solicitudes y analizar las causas de los problemas. Centrar la perspectiva en áreas de solicitud específicas para que dichos estudios puedan resultar más significativos y reveladores.

Las siguientes áreas de solicitud predefinidas se instalan con CA Service Desk Manager:

- Aplicaciones
- Correo electrónico
- Hardware

- Redes
- Impresora
- Software

El software se subdivide en varias áreas de solicitud.

Nota: Para obtener más información sobre cómo definir y editar áreas de solicitud, consulte la *ayuda en línea*.

Más información:

[Propiedades del área de solicitud/incidente/problema](#) (en la página 293)

[Definición de áreas de petición/incidente/problema para el autoservicio](#) (en la página 295)

Propiedades del área de solicitud/incidente/problema

Las propiedades se pueden usar para agregar cualidades o atributos personalizados a un área de solicitud específica. Si ha agregado propiedades a un área de solicitud, cuando un analista le asigna un ticket a ésta, las propiedades asociadas aparecen automáticamente en la ficha Propiedades del ticket. Por ejemplo, puede agregar propiedades al área de solicitud de correo electrónico predefinida para especificar el tamaño del buzón de correo o el servidor de correo electrónico.

Conforme define propiedades, puede especificar si un valor es obligatorio u opcional. En el caso de propiedades con un valor obligatorio (see page 294), los usuarios deben introducir un valor (o aceptar el valor predeterminado) para poder guardar el ticket.

La opción `keep_tasks` determina lo que sucede si se asigna un ticket existente a un área de solicitud diferente:

- Si no está instalada `keep_tasks`, las propiedades existentes (y las tareas de workflow) se eliminan del ticket y se agrega cualquier propiedad o tarea asociada a la categoría nueva.
- Si no está instalada `keep_tasks`, las propiedades existentes y las tareas se retienen en el ticket y se agrega cualquier propiedad o tarea asociada a la solicitud nueva.

Nota: Para obtener instrucciones pormenorizadas sobre cómo agregar propiedades a un área de solicitud y definir reglas de validación de propiedades, consulte la *Ayuda en línea*.

Reglas de validación de propiedades

Puede definir reglas de validación para limitar los valores de propiedad que los usuarios pueden introducir en un conjunto predefinido de valores seleccionables. Por ejemplo, si ha definido una propiedad llamada Sistema operativo, puede definir la regla de validación como una lista desplegable que contenga las opciones Windows, UNIX y Linux.

Las propiedades definidas sin reglas de validación se presentan al usuario como cuadros de texto de formato libre, lo cual permite introducir cualquier cadena de texto. Las reglas de validación hacen que el suministro de información sobre un área y los valores de las categorías sea menos complejo y proclive a que se produzcan errores.

Nota: Las reglas de validación de propiedades se pueden reutilizar. No son específicas de una propiedad en particular. Se puede aplicar cualquier regla de validación existente a las propiedades de categorías de cambios, categorías de incidencias o áreas de solicitud/incidente/problema.

Dependiendo del tipo de regla de validación que haya configurado para una propiedad, cuando el usuario asigne un ticket a la categoría o el área a la que se encuentra adjunta dicha propiedad, aparecerá uno de los controles siguientes en la ficha Propiedades del ticket:

- Cuadro de edición de texto: no se ha definido ninguna regla de validación y no se puede especificar ningún valor predeterminado. Se espera que los usuarios introduzcan valores que sigan los ejemplos proporcionados.
- Casilla de verificación: aparece una casilla de verificación de dos estados en la ficha Propiedades. De forma predeterminada, la casilla de verificación no está activada. El usuario puede aceptar el valor predeterminado, o seleccionar la casilla de verificación. Las casillas activadas aparecen en la página Detalles del ticket con la indicación Sí en la columna de valor. Las casillas desactivadas aparecen con la indicación No en la columna de valor.
- Lista desplegable: aparece una lista desplegable que contiene un conjunto predefinido de opciones en la ficha Propiedades. Si ha definido un valor predeterminado, éste aparece seleccionado cuando se abre por primera vez la lista desplegable. La opción que selecciona el usuario aparece en la columna de valor de la página de detalles del ticket.

Definición de áreas de petición/incidente/problema para el autoservicio

La opción Autoservicio incluido permite definir qué áreas de petición/incidente/problema se han de incluir en los tickets del autoservicio. También puede definir símbolos de autoservicio diferentes a los que ve el analista. Cuando se guarda el ticket, el símbolo de autoservicio se muestra en el campo Área de petición/incidente/problema. Si el ticket se muestra en la interfaz del analista, aparece el símbolo normal para el área. Al usuario de autoservicio no se le permite editar el símbolo, ya que es de sólo lectura.

Para definir un área de petición/incidente/problema para el autoservicio

1. En la ficha Administración, seleccione Service Desk, Peticiones/incidentes/problemas, Áreas.
Aparece la lista de áreas de peticiones/incidentes/problemas.
2. Seleccione Editar en lista
La parte superior de la página muestra los campos editables.
3. Abra el área de petición/incidente/problema deseada para editarla en la lista Símbolo (Hardware.pc.install, por ejemplo).
4. Rellene los siguientes campos:

Autoservicio incluido

Especifica si esta área de petición/incidente/problema se muestra en la interfaz de autoservicio.

Símbolo de autoservicio

Define un identificador exclusivo para esta área de petición/incidente/problema en la interfaz de autoservicio.

Activo

Especifica si el área de petición/incidente/problema está activa o inactiva.

El autoservicio define el área de petición/incidente/problema.

5. Haga clic en Guardar.

La nueva área de petición/incidente/problema aparece en la lista de áreas de petición/incidente/problema cuando se vuelve a mostrar la lista.

Orden de cambio y categorías de incidencia

Las categorías de cambio y las categorías de incidencia definen las agrupaciones lógicas en las cuales se pueden organizar órdenes de cambio e incidencias.

Nota: A diferencia de las áreas de solicitud/incidente/problema, las categorías de órdenes de cambio y las categorías de incidencias se gestionan por separado:

- Configure las categorías de cambios para los modelos de CA Service Desk Manager combinado e interno.
- Configure las categorías de incidencias para los modelos de CA Service Desk Manager combinado y externo.

Las categorías sirven para especificar valores predeterminados para ciertos campos de los partes. Es posible asociar de forma automática niveles de servicio a los partes mediante la asignación de tipos de servicios predeterminados a las categorías. Además, también se pueden asociar estudios a las categorías.

En cada categoría, se pueden especificar los atributos o las cualidades que se asociarán al ticket y crear un workflow que identifique todas las tareas individuales necesarias para realizar el ticket. Si se define el comportamiento asociado a las tareas de workflow, es posible notificar a los miembros pertinentes del personal el estado de los cambios de las tareas o a medida que las actividades cierran los tickets.

Siempre que un analista asigna un ticket a una categoría, toda la información que se haya asociado a esa categoría se introducirá automáticamente en el ticket. Por ejemplo, al indicar un tipo de servicio, se asocia al ticket pertinente y a sus eventos de tipo de servicio asociados.

Nota: Para obtener más información sobre cómo definir y editar categorías, consulte la *ayuda en línea*.

Más información:

[Categorías de cambio predefinidas](#) (en la página 297)

[Categorías de incidencia predefinidas](#) (en la página 297)

[Reglas para cambiar las categorías en los partes](#) (en la página 297)

[Propiedades de la categoría](#) (en la página 298)

[Definición de cambio y emisión de categorías para el autoservicio](#) (en la página 301)

Categorías de cambio predefinidas

Los conjuntos siguientes de categorías de cambio predefinidas se instalan con CA Service Desk Manager:

- Agregar
- Cambiar
- Mover
- Retirar

Nota: Todos estos conjuntos de categorías se subdividen en categorías más específicas. Por ejemplo, el conjunto de la categoría Cambio incluye categorías para estaciones de trabajo y servidores cambiantes.

Categorías de incidencia predefinidas

Las categorías de incidencias predefinidas siguientes se instalan con CA Service Desk Manager:

- Hardware.pc.install
- Software.pc.install

Puede establecer el estado de cualquier categoría como activo o inactivo. Cuando haga que una categoría esté como inactiva, ya no estará disponible para ser utilizada por los analistas, pero no se suprime de la base de datos. Si posteriormente decide utilizar la categoría, vuelva a cambiar el estado a activo.

Reglas para cambiar las categorías en los partes

Las reglas siguientes afectan únicamente a las tareas de workflow.

- Si la categoría anterior utilizaba CA Workflow o Classic Workflow y la nueva categoría utiliza CA IT PAM, la definición del proceso CA IT PAM establece un vínculo a un workflow de un servidor CA IT PAM.
- Si tanto las antiguas categorías como las nuevas se sirven del workflow de CA Service Desk Manager, se aplican las reglas de las versiones anteriores.

- Si la nueva categoría utiliza CA Workflow o CA IT PAM y la categoría anterior utilizaba el workflow de CA Service Desk Manager, se produce lo siguiente:
 - Todas las tareas de workflow sin finalizar y pendientes (las que se pueden actualizar) de la versión 6.0 de CA Service Desk Manager se establecen en el estado Cancelado, independientemente de la opción KEEP_TASKS. Las tareas de workflow finalizadas se conservan, pero no se pueden volver a abrir.
 - Todas las tareas incompletas y no activas (por ejemplo las tareas en estado de espera) se suprimen.
 - Se crea una instancia de la definición de CA Workflow o CA IT PAM.
- Si la categoría nueva utiliza el workflow de CA Service Desk Manager y la antigua utiliza CA Workflow o CA IT PAM, se produce lo siguiente:
 - La instancia de CA Workflow o CA IT PAM se establece por la fuerza en el estado Finalizado.
 - Las tareas de workflow de la categoría nueva se agregan del modo habitual.
- Si tanto la categoría anterior como la categoría nueva utilizan CA Workflow, se produce lo siguiente:
 - Si ambas señalan a la misma definición de procesos, continúa la instancia en ejecución de la categoría anterior.
 - Si ambas señalan distintas definiciones de procesos, la instancia anterior se establece en el estado Finalizado y se crean instancias de la definición de la categoría nueva.

En un workflow de CA Service Desk Manager, no se pueden cerrar los tickets que contienen una instancia de CA Workflow o CA IT PAM en ejecución. Las funciones de acumulación, aceleración e inserción de tareas permanecen desactivadas en los tickets que se sirven de CA Workflow.

Propiedades de la categoría

Se utilizan propiedades para agregar cualidades o atributos personalizados a una categoría específica. Si ha agregado propiedades a una categoría, cuando un analista le asigna un ticket a ésta, las propiedades asociadas aparecen automáticamente en la ficha Propiedades del ticket.

Por ejemplo, tal vez quiera agregar propiedades a la categoría de incidencias predefinida Software.pc.install para especificar tamaño de memoria, tipo de procesador, etc.

Conforme define propiedades, puede especificar si un valor es obligatorio u opcional. En el caso de propiedades con un valor obligatorio, los usuarios deben introducir un valor (o aceptar el valor predeterminado) para poder guardar el ticket.

Mantenimiento de las propiedades de categoría

La opción `keep_tasks` determina lo que sucede si se asigna un ticket existente a una categoría diferente:

- Si no está instalada `keep_tasks`, las propiedades existentes y las tareas de workflow se eliminan del ticket y se agrega cualquier propiedad o tarea asociada a la categoría nueva.
- Si no está instalada `keep_tasks`, las tareas y propiedades existentes se conservan en el ticket, y se agrega cualquier propiedad o tarea asociada a la categoría nueva.

Nota: Para obtener instrucciones pormenorizadas sobre cómo agregar propiedades a una categoría de incidencias o cambios y definir reglas de validación de propiedades, consulte la *Ayuda en línea*.

Reglas de validación de propiedades

Puede definir reglas de validación para limitar los valores de propiedad que los usuarios pueden introducir en un conjunto predefinido de valores seleccionables. Por ejemplo, si ha definido una propiedad llamada Sistema operativo, puede definir la regla de validación como una lista desplegable que contenga las opciones Windows, UNIX y Linux.

Las propiedades definidas sin reglas de validación se presentan al usuario como cuadros de texto de formato libre, lo cual permite introducir cualquier cadena de texto. Las reglas de validación hacen que el suministro de información sobre un área y los valores de las categorías sea menos complejo y proclive a que se produzcan errores.

Nota: Las reglas de validación de propiedades se pueden reutilizar. No son específicas de una propiedad en particular. Se puede aplicar cualquier regla de validación existente a las propiedades de categorías de cambios, categorías de incidencias o áreas de solicitud/incidente/problema.

Dependiendo del tipo de regla de validación que haya configurado para una propiedad, cuando el usuario asigne un ticket a la categoría o el área a la que se encuentra adjunta dicha propiedad, aparecerá uno de los controles siguientes en la ficha Propiedades del ticket:

- Cuadro de edición de texto: no se ha definido ninguna regla de validación y no se puede especificar ningún valor predeterminado. Se espera que los usuarios introduzcan valores que sigan los ejemplos proporcionados.

- Casilla de verificación: aparece una casilla de verificación de dos estados en la ficha Propiedades. De forma predeterminada, la casilla de verificación no está activada. El usuario puede aceptar el valor predeterminado, o seleccionar la casilla de verificación. Las casillas activadas aparecen en la página Detalles del ticket con la indicación Sí en la columna de valor. Las casillas desactivadas aparecen con la indicación No en la columna de valor.
- Lista desplegable: aparece una lista desplegable que contiene un conjunto predefinido de opciones en la ficha Propiedades. Si ha definido un valor predeterminado, éste aparece seleccionado cuando se abre por primera vez la lista desplegable. La opción que selecciona el usuario aparece en la columna de valor de la página de detalles del ticket.

Definición de cambio y emisión de categorías para el autoservicio

Puede utilizar la opción Autoservicio incluido para definir qué categorías de cambio e incidencia se deben incluir en los tickets para el autoservicio. También puede definir símbolos de autoservicio diferentes a los que ve el analista. Cuando el ticket se guarda, el símbolo de autoservicio aparece en el campo Categoría de cambio (o incidencia). Si se muestra el ticket en la interfaz del analista, aparece el símbolo normal para la categoría.

Para definir una categoría de cambio (o incidencia) para el autoservicio

1. En la ficha Administración, seleccione Service Desk, Órdenes de cambio (o incidencias), Categorías.

Aparecerá la página Lista de categorías.

2. Seleccione Editar en lista

La parte superior de la página muestra los campos editables.

3. Seleccione la categoría deseada en la lista Símbolo.
4. Rellene los siguientes campos:

Autoservicio incluido

Especifica si esta categoría se muestra en la interfaz de autoservicio.

Predeterminado: Sí

Símbolo de autoservicio

Define un identificador exclusivo para esta categoría en la interfaz de autoservicio.

Activo

Especifica si la categoría está activa o inactiva.

Se define la categoría para el autoservicio.

5. Haga clic en Guardar.

La categoría actualizada aparecerá en la lista de categorías de cambios (o incidencias) cuando se vuelva a mostrar la lista.

Cierre automático de tickets

Puede utilizar una definición configurable para permitir el cierre automático de los tickets (peticiones/incidentes/problemas, órdenes de cambio o incidencias). Cuando se establece un ticket en estado Resuelto, éste se cierra automáticamente en el número especificado de horas de negocio. La notificación de actividad de cierre automático enviada al usuario final muestra el número de horas de negocio que transcurrirán antes de que el ticket se cierre. El número de horas es configurable y específico del cliente. Si se modifica el estado antes de que termine el número configurable de horas, el cierre del ticket se cancela.

Los administradores puede ejecutar las acciones siguientes:

- Defina una configuración de ticket de cierre automático para controlar el número de horas de negocio, para el usuario final, antes de que el ticket se cierre automáticamente.
- Configure una notificación de actividad de cierre automático para notificar a los contactos adecuados cuando se programa el cierre automático para un ticket.

Si utiliza multicliente, considere lo siguiente:

- El sistema utiliza la definición de cierre automático pública predeterminada cuando no se encuentra una definición de cierre automático específica del cliente.
- Hay una definición de cierre automático para cada cliente.

Nota: Para obtener información más detallada sobre cómo ejecutar estos procedimientos, consulte la información sobre las definiciones de cierre automático en la *Ayuda en línea*.

Más información:

[Cómo establecer las definiciones de ticket de cierre automático](#) (en la página 303)

[Cómo definir una notificación de actividad de cierre automático](#) (en la página 304)

Cómo establecer las definiciones de ticket de cierre automático

Puede definir el número de horas comerciales antes de que un ticket se cierre (todos los tipos de ticket) de la siguiente manera:

1. En la ficha Administración, seleccione Service Desk, Datos de la aplicación, Códigos, Cierre automático.
2. Haga clic en Crear nuevo en la página de lista.
3. Rellene los siguientes campos de la página de detalles:

Símbolo

Define el nombre de la definición del sistema.

Incidencia/orden de cambio de solicitud/incidente/problema

Define el número de horas comerciales, después de que el ticket se establezca en el estado Resuelto, antes de que se cierre el ticket. Si se modifica el estado antes de que termine el número de horas, el cierre del ticket se cancela. 0 (cero) horas indica que no se ha implementado el cierre automático para el tipo de ticket.

Descripción

Ofrece una descripción breve del registro.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Indica si el registro está activo o inactivo.

Se define la configuración del cierre automático.

4. Haga clic en Guardar, Cerrar ventana.

La nueva definición aparece en la página Lista de cierre automático cuando vuelve a visualizar la lista.

Cómo definir una notificación de actividad de cierre automático

Puede cambiar las definiciones en la notificación de actividad de cierre automático predeterminada para notificar a los contactos apropiados cuando se programa el cierre automático para un ticket. La actividad es válida para todos los tipos de ticket de CA Service Desk Manager e incluye una regla de notificación predeterminada para peticiones/incidentes/problemas, órdenes de cambio e incidencias.

Para definir una notificación de actividad de cierre automático, realice lo siguiente:

1. En la ficha Administración, seleccione Notificaciones, Notificaciones de actividades.
2. Seleccione la notificación de actividad de cierre automático en la página de lista para abrirla.
3. Actualice la regla de notificación predeterminada de cierre automático y especifique los contactos que recibirán notificaciones.
4. Haga clic en Guardar, Cerrar ventana.

La notificación de actividad de cierre automático actualizada aparecerá en la lista de notificaciones de actividades cuando se vuelva a mostrar la lista.

Actividades del ticket relacionado

Cuando se genera una actividad para un ticket de CA Service Desk Manager, puede propagar la actividad a uno o más tickets relacionados. Por ejemplo, un registro de problema creado a partir de un incidente puede actualizar el registro de incidentes cuando se resuelve el problema. Cuando se produce la actividad, se genera un registro de actividades para el ticket relacionado que incluye la siguiente información:

- Tipo de actividad de ticket relacionado, por ejemplo Estado de actualización
- Nombre de contacto
- Tipo de ticket principal y su número de referencia
- Descripción del registro de actividades, por ejemplo, estado actualizado desde Trabajo en curso a Abrir

Los registros de actividades se propagan a los tickets relacionados en función del conjunto de propiedades dentro de cada notificación de actividades. Los atributos de los tickets relacionados no se modifican. Se propagan las siguientes relaciones:

- Los problemas se propagan a todos los incidentes activos.
- Las órdenes de cambio se propagan a todos los problemas e incidentes activos.

Como administrador del sistema, puede ejecutar las siguientes acciones:

- Establezca notificaciones de actividad para propagar actividades de tickets relacionados.
- Configure una notificación de actividad de ticket relacionado para notificar a los contactos apropiados cuando la actividad se propague a tickets relacionados.

Nota: Para obtener información más detallada sobre cómo realizar estos procedimientos, consulte la información sobre notificaciones de actividad en la *Ayuda en línea*.

Más información:

[Cómo definir notificaciones de actividad para tickets relacionados](#) (en la página 306)

[Cómo definir notificaciones de actividad de tickets relacionados](#) (en la página 307)

Cómo definir notificaciones de actividad para tickets relacionados

Puede propagar registros de actividades a los tickets relacionados en función del conjunto de propiedades de cada notificación de actividades. Los atributos de los tickets relacionados no se modifican.

Para definir una notificación de actividad para actividades de tickets relacionados, realice lo siguiente:

1. En la ficha Administración, seleccione Notificaciones, Notificaciones de actividades.
2. Abra la notificación de actividades apropiada para editarla.
3. En la página de detalles, haga clic en la casilla de verificación Actividad del ticket relacionado para marcarla como activa.

Nota: Si utiliza multicliente, haga lo siguiente:

- Especifique el tipo de cliente apropiado de la lista desplegable Actividad del ticket relacionado.
 - Introduzca el nombre del cliente en el campo de cliente o haga clic en el icono de búsqueda para buscar un cliente.
4. (Opcional) Actualice la regla de notificación predeterminada y especifique los contactos que recibirán notificaciones.
 5. Haga clic en Guardar, Cerrar ventana.

La notificación de actividad actualizada aparecerá en la lista de notificaciones de actividades cuando se vuelva a mostrar la lista.

Cómo definir notificaciones de actividad de tickets relacionados

Puede cambiar la configuración predeterminada en la notificación de actividad del ticket relacionado para notificar a los contactos apropiados cuando los registros de actividades se propagan a tickets relacionados (solicitudes/incidentes/problemas, solicitudes de cambio e incidencias).

Para definir una notificación de actividad de tickets relacionados, realice lo siguiente:

1. Abra la notificación de actividad de tickets relacionados en la página Lista de notificaciones de actividades.
2. Haga clic en Editar y cambie uno o más campos según corresponda en la página de detalles.
3. (Opcional) Actualice la regla de notificación predeterminada y especifique los contactos que recibirán notificaciones.
4. Haga clic en Guardar, Cerrar ventana.

La notificación de actividad de ticket relacionado aparecerá en la lista de notificaciones de actividades cuando se vuelva a mostrar la lista.

Cálculo de prioridad

El *cálculo de prioridad* es un conjunto predefinido de valores que establece automáticamente los campos Prioridad, Urgencia e Impacto de problemas e incidentes.

Al instalar esta versión de CA Service Desk Manager, un cálculo de prioridad predeterminado gestiona automáticamente los valores de ticket. Se puede modificar la configuración del cálculo de prioridad predeterminado o crear cálculos de prioridad adicionales para gestionar incidentes o problemas. En el caso del multicitiente, tanto usted como los clientes pueden crear cálculos de prioridad adicionales con una configuración específica para cada cliente.

En el cálculo de prioridad, puede definir el resultado en función de los escenarios de negocio para hacer más congruentes el nivel de importancia y el tratamiento de tickets. Los usuarios pueden sustituir algunas definiciones, pero ya no pueden establecer la Prioridad en el ticket porque este valor se controla por medio de datos.

Nota: Si migró desde una versión anterior, el cálculo de prioridad está deshabilitado de manera predeterminada. Para obtener información sobre cómo habilitar el cálculo de prioridad o conservar las personalizaciones, consulte la *Guía de implementación*.

Cuando un analista abre un incidente o un problema, el sistema utiliza automáticamente un cálculo de prioridad activo y valores de ticket para generar la configuración de Prioridad, Urgencia e Impacto. La configuración se basa en uno o más de los siguientes campos:

- Urgencia
- Impacto
- Usuario final afectado
- Área de problema o incidente
- Fecha de apertura
- Servicio afectado

Los analistas pueden sustituir los valores de urgencia e impacto según sea necesario. Según cómo configure el Gestor de opciones, los empleados pueden sustituir solamente valores de urgencia de incidentes cuando la opción *urgency_on_employee* está instalada. Cuando el indicador de motivo de captura está habilitado y los usuarios sustituyen valores de urgencia o impacto y hacen clic en Guardar, aparece la página Escalar detalles que permite a los usuarios describir una razón para el cambio.

Todos los cálculos de prioridad de ticket, sustituciones manuales e información de motivos aparecen en el nuevo registro de actividades. Si no se produce ningún ajuste de cálculo de prioridad, el sistema no crea una entrada de registro de actividades.

Cómo gestiona el cálculo de prioridad los valores de ticket

El sistema ajusta los valores de problema e incidente en función de la configuración del cálculo de prioridad activo para ayudar a los analistas a tratar los tickets de manera más eficaz. La siguiente tabla resume cómo el cálculo de prioridad cambia los campos en función del cálculo de prioridad y las acciones de usuario para problemas, incidentes, servicio Web, correo electrónico y Text API:

Acción	Cambios de campo automáticos	Descripción
El usuario cambia el servicio afectado	Impacto Prioridad	El sistema evalúa el valor de impacto del servicio en el elemento de configuración del tipo de servicio para calcular el nuevo valor de impacto. Los elementos de configuración del tipo de servicio se definen como elementos de configuración con su clase definida en la familia Servicio de empresa. Si la fecha abierta del ticket está dentro del marco de

Acción	Cambios de campo automáticos	Descripción
		tiempo de la ventana de desactivación, el sistema incrementa un nuevo valor de impacto en función del campo Incremento del impacto. El sistema solamente reemplaza el valor de impacto cuando el nuevo valor es mayor que el valor de impacto inicial.
El usuario cambia el área de incidente	Urgencia	El valor de urgencia cambia solamente cuando el nuevo valor es mayor que el valor predeterminado.
El usuario cambia el área de incidente y el usuario final afectado	Urgencia Prioridad	Si el usuario establece primero el campo de área de incidente, el valor de urgencia cambia después de que el usuario establece el usuario final afectado. El cálculo de prioridad establece la prioridad.
El usuario cambia la urgencia y el impacto	Prioridad Impacto	El sistema evalúa el valor de impacto del servicio en el elemento de configuración del tipo de servicio para calcular el nuevo valor de impacto. Si la fecha abierta del ticket está dentro de un intervalo de tiempo definido por la ventana de desactivación, el sistema incrementa un nuevo valor de impacto en función del campo Incremento del impacto. El sistema solamente reemplaza el valor de impacto cuando el nuevo valor es mayor que el valor de impacto inicial. Si el administrador establece el Motivo de captura, el usuario debe proporcionar una razón para la modificación. Si el usuario cambia los valores de urgencia o de impacto, estos valores siguen siendo los mismos en todo el proceso de creación de tickets o actualización de tickets a menos que el usuario los modifique otra vez. Sin embargo, el sistema puede actualizar los valores sustituidos por urgencia o impacto la próxima vez que el usuario actualice el ticket. Después de que el sistema ajusta la urgencia y el impacto, el cálculo de prioridad establece el valor de prioridad.
El usuario selecciona el nuevo incidente en función del documento de conocimiento y el sistema tiene sustituciones para los	Impacto Urgencia	El sistema siempre utiliza los valores de solución de conocimiento o documento de conocimiento independientemente de si los valores son mayores o menores que los valores predeterminados del

Acción	Cambios de campo automáticos	Descripción
documentos de conocimiento (see page 317)		cálculo de prioridad. Por ejemplo, si un cálculo de prioridad tiene un valor de impacto de 3-Un sólo grupo y un valor de urgencia de 3-Rápido, y los documentos de conocimiento tienen un valor de impacto de 2-Varios grupos y un valor de urgencia de 4-Muy rápido, el sistema aplica los valores del documento de conocimiento al incidente. El valor de prioridad siempre se deriva del cálculo de prioridad.
El usuario acepta el documento de conocimiento como solución para el problema o incidente	Impacto Urgencia	El sistema utiliza los valores del documento de conocimiento para impacto y urgencia. El sistema también utiliza el cálculo de prioridad para establecer el valor de prioridad.
El usuario obtiene el incidente del documento de conocimiento al seleccionar Nuevo incidente	Impacto Urgencia Prioridad	El sistema utiliza los valores del cálculo de prioridad.
El usuario obtiene el incidente del documento de conocimiento sin sustituciones del sistema para documentos de conocimiento (see page 317)	Impacto Urgencia Prioridad	El sistema utiliza los valores del cálculo de prioridad independientemente de la forma en que el usuario creó el incidente para el documento de conocimiento o solución de conocimiento.
El ticket acepta el documento de conocimiento como solución para el problema o incidente, y el sistema no sustituye documentos de conocimiento	Impacto Urgencia Prioridad	El sistema utiliza valores del problema o incidente. El valor de prioridad proviene del cálculo de prioridad.
El ticket que está en modo de sólo lectura acepta el documento de conocimiento como solución para el problema o incidente, y el sistema sustituye documentos de conocimiento	Impacto Urgencia Prioridad	El sistema utiliza valores de impacto y urgencia del documento de conocimiento si los valores no están vacíos. Si el valor de impacto o urgencia en el documento de conocimiento está vacío, el sistema utiliza valores del problema o incidente. El valor de prioridad proviene del cálculo de prioridad.
El ticket que está en modo de edición acepta el documento de conocimiento	Impacto Urgencia	El sistema utiliza valores del problema o incidente. El valor de prioridad proviene del cálculo de prioridad.

Acción	Cambios de campo automáticos	Descripción
como solución para el problema o incidente, y el sistema sustituye documentos de conocimiento.	Prioridad	

Cómo establecer el cálculo de prioridad

De forma predeterminada, los valores de ticket como la prioridad se basan en un cálculo de prioridad. Puede encontrar y ajustar los valores iniciales para prioridad y urgencia en web.cfg. web.cfg tiene definiciones separadas para diversos usuarios como invitados, usuarios VIP y empleados.

Nota: Si migró desde una versión anterior, el cálculo de prioridad está deshabilitado de manera predeterminada. Las páginas de detalles de problemas e incidentes personalizados requieren una configuración adicional para funcionar correctamente. Para obtener información sobre cómo habilitar el cálculo de prioridad o conservar las personalizaciones, consulte la *Guía de implementación*.

Para establecer este cálculo de prioridad, realice lo siguiente:

1. En la ficha Administración, seleccione Service Desk, Solicitudes/incidentes/problemas, Cálculo de prioridad.
Aparecerá la lista Cálculo de prioridades.
2. Haga clic con el botón derecho del ratón en el cálculo de prioridad predeterminado y seleccione Editar en el menú contextual.

La página Detalles de cálculo de prioridad predeterminada muestra definiciones predeterminadas para tickets de incidente y problema.

3. Revise el cálculo de prioridad predeterminado y ajuste los valores en consecuencia. Cuando establezca los valores de cálculo de prioridad, considere las siguientes incidencias para su entorno de trabajo:
 - **Escalación de incidencia:** cuando los tickets requieren escalación a un VIP particular, puede aumentar el valor de urgencia.
 - **CI graves:** para CI graves, puede configurar el impacto de servicio para cada CI.
 - **Tiempo de disponibilidad de servicio crítico:** cuando los CI requieren de disponibilidad alta, agregue una ventana de desactivación.
 - **Ventana de desactivación:** cuando los tickets relacionados con CI utilizan una ventana de desactivación particular, puede aumentar el valor del impacto del servicio en el cálculo de prioridad.
4. Utilice la configuración de anulación manual para permitir a los usuarios que cambien las definiciones de tickets como sea necesario.
5. Si quiere un cálculo de prioridad separado para gestionar, problemas o incidentes, configure el tipo de ticket (see page 314).
6. Haga clic en Guardar.

En el siguiente ticket nuevo o actualizado o documento de conocimiento, los campos se actualizan según los valores del cálculo de prioridad activo.
7. Considere crear cálculos de prioridad adicionales para cada tipo de ticket. En el caso de multicientes, cree y active cálculos de prioridad adicionales para gestionar tickets para cada cliente.

Nota: Para obtener información sobre el cálculo de prioridad, consulte la *Ayuda en línea*.

Varios cálculos de prioridad

Puede establecer más de un cálculo de prioridad. Sin embargo, solamente un cálculo de prioridad activo trata problemas, incidentes o ambos. Por ejemplo, puede tener un cálculo de prioridad activo para problemas y otro para incidentes. También puede guardar varios cálculos de prioridad inactivos para su uso futuro.

Asignación de cálculo de prioridad para el multicitiente

Usted o sus clientes pueden crear cálculos de prioridad específicos de cliente para gestionar incidentes y problemas. Cuando asigna cálculos de prioridad para el multicitiente, tenga en cuenta lo siguiente:

- Cuando un cálculo de prioridad no tiene ningún cliente asignado, se considera público. El estado de un cálculo de prioridad público es activo o inactivo. Un cálculo de prioridad deja de considerarse público cuando se le asigna a un cliente.
- Si un cliente no tiene ninguna asignación de cálculo de prioridad, el cálculo de prioridad predeterminado u otro cálculo de prioridad público y activo gestiona automáticamente problemas e incidentes.
- Un cálculo de prioridad gestiona problemas e incidentes para un cliente. Sin embargo, un cálculo de prioridad específico de cliente puede tratar por separado cada tipo de ticket. Por ejemplo, la compañía X tiene un cálculo de prioridad para tratar incidentes y otro para gestionar problemas.
- Cuando los clientes crean sus propios cálculos de prioridad mientras los cálculos de prioridad públicos están activos, el cálculo de prioridad específico de cliente se aplica solamente a los tickets para el cliente respectivo.

Por ejemplo, si el cálculo de prioridad predeterminado está activo, el cliente de la compañía X puede crear un cálculo de prioridad específico de cliente denominado `new_priority_calculation`. La configuración de `new_priority_calculation` se aplica solamente a problemas e incidentes de la compañía X.

- Si el cliente desactiva un cálculo de prioridad, el sistema utiliza un cálculo de prioridad público activo para gestionar incidentes y problemas de clientes.

Por ejemplo, la compañía X desactiva el cálculo de prioridad específico de cliente mientras todavía hay un cálculo de prioridad predeterminado activo. El cálculo de prioridad permanece habilitado para la compañía X porque el sistema utiliza el cálculo de prioridad predeterminado para gestionar los incidentes y problemas de dicha compañía.

Nota: Dado que los clientes pueden suprimir sus propios registros de cálculo de prioridad, se recomienda desactivar los cálculos de prioridad públicos que gestionan incidentes y problemas. En cambio, usted o los clientes pueden crear cálculos de prioridad específicos de cliente.

- Cuando deshabilite el multicitiente y haya más de un cálculo de prioridad activo que gestiona clientes, deje *solamente un* cálculo de prioridad para gestionar incidentes y problemas. Por ejemplo, puede desactivar todos los cálculos de prioridad excepto uno para gestionar incidentes y otro para tratar problemas.

Nota: Para obtener información acerca del multicitiente, consulte la *Guía de implementación*.

Cómo asignar clientes a un cálculo de prioridad

En el caso del multicitiente, puede asignar clientes a un cálculo de prioridad. Primero, desactive los cálculos de prioridad públicos. A continuación, asigne el cliente a un cálculo de prioridad y actívelo.

Para asignar un cliente a un cálculo de prioridad, realice lo siguiente:

1. En la ficha Administración, seleccione Service Desk, Solicitudes/incidentes/problemas, Cálculo de prioridad.
Aparecerá la lista Cálculo de prioridades.
2. Edite cada cálculo de prioridad público, como el predeterminado.
Establezca el estado en inactivo y haga clic en Guardar.
El sistema deshabilita los cálculos de prioridad públicos.
3. Para cada cliente, cree o edite un cálculo de prioridad con configuración específica de cliente para Impacto, Urgencia y Prioridad.
Aparece la página Crear cálculo de prioridad o Actualizar cálculo de prioridad.
4. En el campo Nombre, especifique el cliente.
5. En el campo Estado, seleccione Activo.
6. Haga clic en Guardar.
El sistema aplica valores específicos de cliente para Impacto, Urgencia y Prioridad en nuevos incidentes y problemas.

Nota: Para obtener información sobre cómo crear y editar cálculos de prioridad, consulte la *Ayuda en línea*.

Consideraciones de tipo de ticket para el cálculo de prioridad

Cuando configure tipos de ticket para un cálculo de prioridad, tenga en cuenta lo siguiente:

- El cálculo de prioridad predeterminado permite gestionar tipos de ticket de incidente y de problema.

- Si está migrando de una versión anterior, puede habilitar el cálculo de prioridad predeterminado o crear un cálculo de prioridad para gestionar problemas e incidentes.
- Aunque puede tener muchos cálculos de prioridad, solamente un cálculo de prioridad activo puede tratar un tipo de ticket particular. Por ejemplo, un cálculo de prioridad activo puede gestionar problemas y otro puede gestionar incidentes.
- Si desea crear un cálculo de prioridad y un cálculo de prioridad activo ya trata un tipo de ticket particular, primero deshabilite el tipo de ticket en el cálculo de prioridad activo. Por ejemplo, si desea que un cálculo de prioridad gestione problemas, puede deshabilitar el tipo de ticket de problema en el cálculo de prioridad activo y crear un cálculo de prioridad activo que gestione problemas.

Nota: Para obtener información sobre cómo habilitar el cálculo de prioridad y cómo configurar tipos de ticket durante la migración, consulte la *Guía de implementación*.

Configuración de tipos de ticket para un cálculo de prioridad

Puede especificar los tipos de ticket que el cálculo de prioridad gestiona. Cuando el cálculo de prioridad está activo, gestiona valores de prioridad, impacto y urgencia en los nuevos tickets.

Procedimiento para configurar tipos de ticket para un cálculo de prioridad

1. En la ficha Administración, seleccione Service Desk, Solicitudes/incidentes/problemas, Cálculo de prioridad.
Aparecerá la lista Cálculo de prioridades.
2. Haga clic con el botón secundario en un cálculo de prioridad y seleccione Editar.
Aparecerá la página Actualizar cálculo de prioridad.
3. Active o desactive una o más de las siguientes opciones:

Incidentes

Habilita o deshabilita el cálculo de prioridad para gestionar nuevos incidentes.

Problemas

Habilita o deshabilita el cálculo de prioridad para gestionar tickets de problemas nuevos.

4. Haga clic en Guardar.

CA Service Desk Manager utiliza la configuración del cálculo de prioridad para gestionar valores de ticket para nuevos incidentes, problemas o ambos.

Uso de plantillas de ticket para calcular valores de prioridad

Si desea que las plantillas de ticket calculen la prioridad, puede configurar el cálculo de prioridad con la opción *Activado para plantillas*. Si habilita esta opción los valores de urgencia e impacto proceden de la plantilla, pero el campo de prioridad procede del registro de cálculo de prioridad. El valor de prioridad se muestra como de sólo lectura.

Si no habilita esta opción, los campos de urgencia, impacto y prioridad proceden de la plantilla. Puede editar el campo de prioridad y no se realizará ningún cálculo de prioridad para el ticket hasta que se guarde.

Procedimiento para utilizar plantillas de ticket para calcular valores de prioridad

1. En la ficha Administración, seleccione Service Desk, Solicitudes/incidentes/problemas, Cálculo de prioridad.
Aparecerá la lista Cálculo de prioridades.
2. Seleccione el cálculo de prioridad que desea utilizar para calcular la prioridad con plantillas.
También puede crear un cálculo de prioridad para utilizar plantillas de ticket para calcular valores de prioridad.
3. Seleccione *Activado para plantillas* en la lista Opciones de cálculo de prioridad.
4. Haga clic en Guardar.
Se habilita la opción.

Utilización de documentos de conocimiento para calcular valores de prioridad

Si quiere que los documentos de conocimiento calculen la prioridad, puede actualizar la asignación de campo. Después de que configure la asignación de campo, el analista puede crear tickets de problema o incidente de documentos de conocimiento. El documento de conocimiento calcula los valores de impacto y urgencia en los tickets. Si falta el valor de impacto o urgencia, los valores provienen del cálculo de prioridad.

Importante: Si modifica y guarda un ticket que ya contiene valores de impacto y urgencia calculados por un documento de conocimiento, el cálculo de prioridad anula los valores establecidos por Gestión del conocimiento. El registro de auditoría muestra estas actividades.

Para utilizar documentos de conocimiento para calcular valores de prioridad

1. En la ficha Administración, seleccione Conocimiento, Integración de Service Desk.
2. Seleccione Asignación de campos.
Aparecerá la página Asignación de campos.
3. Para Impacto y Urgencia, seleccione las siguientes casillas de verificación como sea apropiado:

Rellenar los valores de Service Desk vacíos

Especifica si se debe utilizar la información de Gestión del conocimiento para rellenar los campos en las incidencias o peticiones.

Sobrescribir valores de Service Desk

Identifica los campos de las incidencias o solicitudes que se corresponden con los campos que aparecen en la columna de Gestión del conocimiento.

Nota: Cuando el campo Sobrescribir valores de Service Desk no está habilitado pero el campo Rellenar los valores de Service Desk vacíos está habilitado para Impacto y Urgencia, los valores de conocimiento para Impacto y Urgencia omiten los valores de incidente.

4. Haga clic en Guardar.

Se crean los incidentes y problemas, con los valores de impacto y urgencia del documento de conocimiento para calcular el valor de prioridad. Si faltan los valores, el ticket los obtiene de un cálculo de prioridad activo. Si ningún cálculo de prioridad está activo para un tipo de ticket, el sistema borra los campos Prioridad, Urgencia e Impacto.

Anulación manual del valor de impacto

Cuando se anula manualmente el valor de impacto en un problema o incidente, el cálculo de prioridad activo que gestiona el tipo de ticket automáticamente ajusta el valor de prioridad.

Para anular manualmente el valor de impacto

1. Abra la página de detalles para el problema o incidente que quiera cambiar.
2. Cambie el valor de impacto.

Si hay un cálculo de prioridad activo que gestiona el tipo de ticket, el valor de prioridad cambia automáticamente en función de la configuración en el cálculo de prioridad.

3. Guarde el incidente.

El registro de actividades en la página Detalles de incidente refleja los cambios al valor de impacto.

Ejemplo: anulación manual del valor de impacto en un incidente nuevo

1. Cree un incidente.

De forma predeterminada, el valor de urgencia es 3-Rápido. El valor de impacto es 3-Un solo grupo. El valor de prioridad es 3.

2. Anule el valor de impacto y reemplácelo por 1-Toda la organización.

El valor de prioridad cambia automáticamente en función de los valores en el cálculo de prioridad activo que gestiona incidentes.

3. Guarde el incidente.

El registro de actividades en la página Detalles de incidente refleja los cambios al valor de impacto.

Sustitución manual del valor de urgencia

Cuando se sustituye manualmente el valor de urgencia en un ticket, el cálculo de prioridad activo que gestiona el tipo de ticket ajusta automáticamente el valor de prioridad.

Procedimiento para sustituir manualmente el valor de urgencia

1. Abra la página de detalles para el incidente que desea cambiar.
2. Cambie el valor de urgencia.

Si hay un cálculo de prioridad activo que gestiona el tipo de ticket, el valor de prioridad cambia automáticamente en función de la configuración en el cálculo de prioridad.

3. Guarde el incidente.

El registro de actividades en la página Detalles de incidente refleja los cambios de valores de urgencia.

Ejemplo: sustitución manual del valor de urgencia en un nuevo incidente

1. Cree un incidente.

De forma predeterminada, el valor de urgencia es 3-Rápido. El valor de impacto es 3-Un solo grupo. El valor de prioridad es 3.

2. Sustituya el valor de urgencia por 5-Inmediatamente.

El valor de prioridad cambia automáticamente en función de los valores en el cálculo de prioridad activo que gestiona incidentes.

3. Guarde el incidente.

El registro de actividades en la página Detalles de incidente refleja el cambio en el valor de urgencia.

Ajuste automáticamente del impacto para un problema o incidente

Para los elementos de configuración definidos con una familia de servicios de empresa, puede ajustar automáticamente el valor del impacto para problemas o incidentes. Cuando selecciona el área del problema o incidente y seleccione un servicio afectado, el impacto se ajusta según las definiciones de impacto del servicio de CI para el cálculo de prioridad y CI de servicios de empresa.

Para ajustar automáticamente el impacto para un problema o incidente

1. Cree un problema o incidente para un CI de tipo de servicio de empresa.
2. Seleccione un servicio afectado.
3. Seleccione un área de problema o incidente.

Si hay un cálculo de prioridad activo que gestiona el tipo de ticket, el valor del impacto cambia basado en el valor de Incremento del impacto (utilizado para la evaluación de impacto de la ventana de desactivación) en el cálculo de prioridad y el valor de impacto del servicio desde el servicio afectado.

Si está utilizando el cálculo de prioridad predeterminado, con una definición del impacto del servicio para el CI del servicio de empresa de 1-Toda la organización, y no se abre el problema o incidente dentro de una ventana de desactivación, el valor de impacto en el problema o incidente se establece en 1 y el valor de prioridad en el ticket se eleva a 2.

4. Guarde el parte.

El registro de actividades en la página Detalles de incidente refleja los cambios al valor de impacto.

Ajuste del impacto para un ejemplo de incidente o problema

El siguiente ejemplo muestra cómo ajustar el impacto para un problema o incidente.

1. Cree un CI de Servicio de empresa denominado CI-APC y establezca la clase como una que se incluya en el servicio de empresa de familia.
Por ejemplo, puede establecer la clase como Otros servicios, Servicio de negocios o Servicio de infraestructuras.
2. En la ficha Servicio en el formulario de detalles de CI, establezca el campo Impacto del servicio en 2-Varios grupos.
3. En la ficha Service Desk, cree un incidente y establezca el Servicio afectado en CI-APC.
4. Guarde el parte.

El campo Impacto en el incidente refleja el valor del impacto de servicio del servicio afectado seleccionado (CI-APC). En este caso, el valor de impacto se establece en 2-Varios grupos.

Nota: Si está utilizando el cálculo de prioridad predeterminado y el ticket actual se crea durante un período de ventana de desactivación, el valor de impacto aumenta en 1 y, en el caso anterior, el valor de impacto se establece en 1-Toda la organización.

Nota: Para obtener información sobre cómo crear elementos de configuración, consulte la Ayuda en línea.

Ajuste automático de urgencia para problemas o incidentes

Para los problemas e incidentes, puede ajustar automáticamente la urgencia y la prioridad especificando un usuario final afectado que requiera de tratamiento especial o especificando un área de incidente/problema que tenga un valor de urgencia de área.

Cuando asigna un tratamiento especial, con la opción Escalar urgencia activada, para un contacto o grupo, un valor de urgencia de área para un área de incidente/problema, el valor de urgencia dentro del problema/incidente se ajusta automáticamente según los valores en el cálculo de prioridad y el valor de urgencia de área para el usuario final afectado.

Para ajustar automáticamente la urgencia para un problema o incidente

1. Cree un problema o incidente.
2. Seleccione un usuario final afectado. En caso de una urgencia elevada, seleccione un usuario final afectado que requiera tratamiento especial que tenga activada la opción Escalar urgencia.

Si hay un cálculo de prioridad activo que gestiona el tipo de ticket, el valor de urgencia cambia en función del valor de incremento de la urgencia en el cálculo de prioridad activo.

3. Seleccione un área de problema o incidente.

Si hay un cálculo de prioridad activo que gestiona el tipo de ticket, el valor de urgencia cambia basado en el valor de urgencia de área en la definición del área de incidente/problema.

4. Guarde el parte.

Un mensaje de confirmación le recuerda que el ticket requiere de tratamiento especial. El registro de actividades en la página Detalles de incidente/problema refleja los cambios del valor de urgencia.

Ajuste de la urgencia para un ejemplo de incidente o problema

El siguiente ejemplo muestra cómo ajustar la urgencia para un problema o incidente.

1. En la ficha Administrador, cree un contacto denominado No VIP.
2. Cree un contacto de tratamiento especial denominado VIP y active el valor Escalar urgencia.
3. Cree un área denominada Área de prueba y especifique la urgencia del área como 2-Muy rápido.
4. En la ficha Service Desk, cree un incidente.
5. En el caso del usuario final afectado, seleccione No VIP.
6. En el área de incidente, seleccione Área de prueba y guarde el ticket.

El campo Urgencia refleja el valor de urgencia del área en la definición de área de incidente. En este caso, la urgencia se establece en 2-Muy rápido.

7. Cambie el usuario final afectado a VIP y guarde el ticket.

Si se está utilizando la matriz de cálculo de prioridad, el valor de urgencia aumenta en 1 y se establece en 1-Inmediatamente. Aparece un mensaje de confirmación que le recuerda que el ticket requiere tratamiento especial. El registro de actividades en la página Detalles de incidente refleja los cambios en el valor de urgencia.

Nota: Para obtener información sobre cómo crear contactos y áreas, consulte la *Ayuda en línea*.

Controles de atributo dependiente y transiciones de estado

Puede utilizar los siguientes controles configurables con el fin de restringir los flujos de estado de tickets para solicitudes de cambio, incidencias, incidentes/problemas/solicitudes, así como para determinar los campos que se muestran o que son necesarios para cada estado de ticket:

Transiciones

Controlan el modo en que los usuarios seleccionan los estados disponibles en el incidente/problema/solicitud, la incidencia o el formulario de orden de cambio. Por ejemplo, un problema está en un estado de abierto y el flujo de transición solamente admite que el analista actualice el estado a Cerrado. En este ejemplo, el analista no tiene ninguna otra opción de estado, lo cual refuerza el proceso de gestión de problemas.

Las transiciones permiten definir un subconjunto de la lista completa de estados y especificar el nuevo (o siguiente) estado predeterminado de un ticket en función del estado actual. Puede definir transiciones de estado exclusivas para cada tipo de ticket. Considere la posibilidad de usar transiciones cuando desee restringir workflows para sus usuarios finales.

Atributos dependientes

Controla el modo en que se designan los atributos como necesarios (se deben proporcionar) o bloqueados (no se pueden actualizar) según el estado del ticket. Por ejemplo, el gestor de cambios puede impedir que un analista edite el atributo Resumen después de la aprobación de una orden de cambio. Considere la posibilidad de usar controles de atributo cuando desee restringir ciertos atributos en función del estado.

Nota: Puede especificar el rigor con el que el sistema exige las políticas de estado, si configura la opción de incumplimientos de política de estado en el Gestor de opciones (Opciones generales). Esta opción solamente se aplica a procesos automatizados de sistema, como integraciones y macros.

Más información:

[Cómo trabajar con transiciones de estado y controles de atributo dependiente](#) (en la página 325)

[Configuración de transiciones de estado](#) (en la página 325)

[Configuración de controles de atributo dependiente](#) (en la página 327)

[Métodos de servicios Web](#) (en la página 328)

[Flujos de transición predefinidos](#) (en la página 329)

[Procedimiento recomendado: transiciones de estado predefinidas](#) (en la página 333)

Cómo trabajar con transiciones de estado y controles de atributo dependiente

Para trabajar con transiciones de estado y controles de atributo dependiente, realice lo siguiente:

1. En la ficha Administración, configure los roles, contactos y clientes apropiados para su entorno.
2. En el nodo del Centro de servicio al usuario, especifique un tipo de ticket (Orden de cambio, por ejemplo) y seleccione Estado.

La página Lista de estado muestra códigos de estado activos.

3. Edite el código de estado apropiado (Confirmado, por ejemplo) y utilice los controles disponibles en las fichas ubicadas en la parte inferior de la página de detalles del estado del ticket para hacer lo siguiente:

- Configuración de transiciones de estado (see page 325)
- Configuración de controles de atributo dependiente (see page 327)

Nota: Puede configurar transiciones exclusivas y controles de atributo dependiente para cada tipo de ticket.

Configuración de transiciones de estado

Puede configurar un subconjunto de la lista completa de estados y especificar el siguiente estado predeterminado de un ticket en función del estado actual. Se imponen transiciones cuando el estado se cambia en el formulario de detalles del ticket.

Para configurar transiciones de estado

1. Haga clic en la ficha Transiciones al final de la página de detalles del estado del ticket.

La página Lista de transiciones muestra todas las transiciones válidas para el estado.

Nota: Cuando se los configura, los tipos de transiciones vinculados aparecen en la lista Transición de solicitud y Transición de incidente.

2. Haga clic en el botón Actualizar transiciones.

Aparecerá la página Actualizar transiciones de estado de ticket.

3. Configure las casillas de verificación siguientes según sea necesario:

Permitido

Especifica una transición válida para el estado. Utilice esta opción para restringir flujos de trabajo de estado.

Predeterminado

(Opcional) Especifica la transición de estado predeterminada. CA Service Desk Manager aplica la transición predeterminada cuando un usuario hace clic en el botón de la transición predeterminada en el formulario de detalles del ticket, o cuando un usuario (incluido el usuario de servicios Web) actualiza el estado a un valor <d>. Hay solamente una transición predeterminada para cada estado (o una para cada cliente en un sistema multicliente).

Se debe comentar

(Opcional) Especifica que se requiere un comentario de registro de actividades para la transición al cambiar el estado de un ticket.

Nota: Esta opción sólo se aplica a dispositivos de CA Service Desk Manager. No se aplica a otras áreas, como servicios Web ni la funcionalidad de edición en lista.

4. (Opcional) Seleccione un código de estado en la columna Nombre para actualizar sus detalles.
5. Haga clic en Guardar.

La lista de transiciones configuradas para el nuevo estado aparece en la lista Transición. Cuando el analista selecciona la lista desplegable Estado en el formulario de ticket, aparece la nueva lista de estado.

Nota: Para obtener información detallada sobre el procedimiento de definición de las transiciones de estado, consulte la *Ayuda en línea*.

Configuración de controles de atributo dependiente

Puede determinar los campos mostrados o requeridos para el estado del ticket.

Nota: Antes de que configure los atributos dependientes como "necesarios" para el estado del ticket, tenga en cuenta que la opción Editar en lista que aparece en la página de la lista del ticket puede no mostrar los valores de campo de atributo que se requieren. Si el valor de campo de atributo necesario no es ya parte del ticket guardado, y si no se presenta en el formato Editar en lista, no se guarda el ticket. Por consiguiente, el analista debe editar los valores de campo de atributo dependientes necesarios en la página de detalles del ticket en lugar de utilizar la opción Editar en lista.

Para configurar un control de atributo dependiente

1. En la página de detalles del estado del ticket, seleccione la ficha Control de atributo dependiente en la parte inferior de la página.
Aparecerá la Lista de controles de atributo.
2. Haga clic en Crear.
Aparece la página Actualizar control de atributo dependiente de estado.
3. Rellene los siguientes campos:

Cliente

(Opcional) En un sistema con el multicitiente instalado, especifica un nombre de cliente opcional. Si se especifica un cliente, la dependencia se aplica solamente a ese cliente y a sus subclientes.

Atributo

Especifica el nombre del atributo que quiere controlar, por ejemplo, Resumen.

Bloqueado

Especifica el atributo como bloqueado. Un atributo bloqueado asociado con un estado no se puede actualizar en un ticket con el mismo estado. El atributo se desbloquea cuando se cambia el estado.

Necesario

Especifica el atributo según sea necesario. Un atributo necesario para el estado no puede utilizar un valor nulo en un ticket con el mismo estado.

4. Haga clic en Guardar.

El nuevo control de atributo para el estado aparece en la lista de controles de atributo cuando vuelve a visualizar la página. Cuando un usuario actualiza el estado del ticket, el sistema recupera la lista de atributos necesarios que corresponden al nuevo estado, y actualiza el formulario de ticket como sea apropiado. Aparece un mensaje de error en la parte superior del formulario de ticket cuando un usuario intenta cerrar el ticket sin rellenar un campo necesario.

Nota: Para obtener información detallada sobre el procedimiento de definición de los controles de atributo dependiente, consulte la *Ayuda en línea*.

Métodos de servicios Web

Puede configurar la transición de estado siguiente y los métodos de servicios Web de control de atributo dependiente:

getValidTransitions

Permite a los usuarios listar las transiciones para un ticket. Este método se basa en el método `getValidTaskTransitions` existente, excepto por el hecho de que el argumento puede ser un ticket o un estado.

getDependentAttrControls

Permite a los usuarios listar los atributos bloqueados y necesarios para un atributo de un objeto especificado por el ID persistente. En este momento se admite el atributo de estado.

Nota: Para obtener más información sobre los servicios Web, consulte la *Referencia técnica*.

Flujos de transición predefinidos

Para cada tipo de ticket, puede utilizar las transiciones de estado predefinidas proporcionadas con el producto y modificarlas para alojar su flujo de transición deseado.

Nota: Puesto que se pueden compartir transiciones de estado entre integraciones como CA Workflow, no desactive las transiciones de estado predefinidas a menos que se lo pidan explícitamente.

Para ver la lista de transiciones predefinidas, realice lo siguiente:

En la ficha Administración, amplíe el nodo del Centro de servicio al usuario y seleccione una de las siguientes opciones:

- Transiciones de orden de cambio
- Transiciones de incidencia
- Transiciones de solicitud/incidente/problema

La lista de transiciones muestra las transiciones predefinidas que le permiten controlar cómo continúa un ticket (incidente/petición/problema, orden de cambio e incidencia) a través de su ciclo de vida.

Nota: Para obtener información detallada del proceso de creación y modificación de transiciones, consulte la *Ayuda en línea*.

Flujo de transición de incidente

La tabla siguiente muestra el flujo de transición de incidente predefinido.

Estado actual	Transición predeterminada	Siguientes estados disponibles
Acknowledged (Confirmado)	En curso <d>	Evitado, Esperando distribuidor, Cancelado, Cerrado, Cerrado sin resolver, En curso, Abierto, Cambio pendiente, Resuelto
Evitado		Confirmado, Evitado, Esperando respuesta de usuario final, Cerrado, Cerrado sin resolver, En curso, Rechazar solución, Investigando, Resuelto
Esperando respuesta de usuario final	Investigando <d>	Cerrado, Cerrado sin resolver, En curso, Abierto, Investigando, Resuelto
Esperando distribuidor	Investigando <d>	Confirmado, Cerrado, Cerrado sin resolver, En curso, Abierto, Cambio pendiente, Investigando, Resuelto
Cancelada		Closed (Cerrado)
Closed (Cerrado)		Open (Abierto)

Estado actual	Transición predeterminada	Siguientes estados disponibles
Cerrado y no resuelto		Acknowledged (Confirmado)
Cerrado y no resuelto		Closed (Cerrado)
Cerrado y no resuelto		Open (Abierto)
Hold (En espera)		Confirmado, Cerrado, En curso, Abierto, Cambio pendiente, Resuelto
En curso	Investigando <d>	Confirmado, Esperando respuesta de usuario final, Esperando distribuidor, Cerrado, Cerrado y no resuelto, Abierto, Cambio pendiente, Investigando, Resuelto
Pending Change (Pendiente de cambio)	Investigando <d>	Confirmado, Cerrado, En curso, Abierto, Resuelto
Researching (Investigando)	Resuelto <d>	Cerrado, Abierto, Resuelto
Resuelto	Cerrado <d>	Esperando respuesta de usuario final, Cerrado, Abierto

Flujo de transición de problema

La tabla siguiente muestra el flujo de transición de problema predefinido.

Estado actual	Transición predeterminada	Siguientes estados disponibles
Acknowledged (Confirmado)	En curso <d>	Confirmado, Aprobado, Cancelado, Cerrado, Corrección en curso, Abierto, Rechazado, Investigando
Análisis completo	Aprobado <d>	Confirmado, Cancelado, Cerrado, Corrección en curso
Aprobado	Corrección en curso <d>	Cerrado, Corregido, Cambio pendiente
Esperando distribuidor	Investigando <d>	Confirmado, Cerrado, Cerrado sin resolver, Corregido, En curso, Abierto, Cambio pendiente, Investigando
Cancelada	Cerrado <d>	Cerrado, Cerrado y no resuelto, Abierto
Cerrado y no resuelto		Confirmado, Cerrado, Abierto
Reparación en curso	Corregido <d>	Aprobado, Cancelado, Corregido, Corrección en curso, Investigando, Rechazado

Estado actual	Transición predeterminada	Siguientes estados disponibles
Fijo	Cerrado <d>	Closed (Cerrado)
Hold (En espera)	Investigando <d>	Confirmado, Cerrado, Corregido, En curso, Abierto, Cambio pendiente, Investigando
En curso	Investigando <d>	Confirmado, Aprobado, Cancelado, Cerrado, Corrección en curso, Cambio pendiente, Rechazado, Investigando
Error conocido	Corrección en curso <d>	Cerrado, Corrección en curso, Corregido
Open (Abierto)	Confirmado <d>	Confirmado, Aprobado, Cancelado, Cerrado, Corrección en curso, En curso, Rechazado, Investigando
Pending Change (Pendiente de cambio)	Corregido <d>	Cerrado, Corregido, Investigando
Rechazado	Cerrado <d>	Cerrado, Cerrado y no resuelto, Abierto
Researching (Investigando)	Análisis completo <d>	Confirmado, Análisis completo, Aprobado, Cancelado, Cerrado, Corrección en curso, Corregido, Rechazado

Flujo de transición de incidencia

La tabla siguiente muestra el flujo de transición de incidencia predefinido.

Estado actual	Transición predeterminada	Siguientes estados disponibles
Acknowledged (Confirmado)	En curso <d>	Esperando respuesta de usuario final, Esperando distribuidor, Cerrado, Cerrado sin resolver, En curso, Abierto, Cambio pendiente, Resuelto
Esperando respuesta de usuario final	Investigando <d>	Confirmado, Cerrado, Cerrado sin resolver, En curso, Abierto, Investigando, Resuelto
Esperando distribuidor	Investigando <d>	Confirmado, Cerrado, En curso, Abierto, Cambio pendiente, Investigando, Resuelto
Cancelada	Cerrado <d>	Closed (Cerrado)
Closed (Cerrado)		Confirmado, Abierto
Cerrado y no resuelto		Confirmado, Cerrado, Abierto
Hold (En espera)		Confirmado, Cerrado, En curso, Abierto, Cambio pendiente, Resuelto

Estado actual	Transición predeterminada	Siguientes estados disponibles
En curso	Investigando <d>	Confirmado, Esperando respuesta de usuario final, Esperando distribuidor, Cerrado, Cerrado y no resuelto, Abierto, Cambio pendiente, Investigando, Resuelto
Open (Abierto)	Confirmado <d>	Confirmado, Evitado por autoservicio, Esperando respuesta de usuario final, Esperando distribuidor, Cerrado, Cerrado sin resolver, En curso, Cambio pendiente, Resuelto
Pending Change (Pendiente de cambio)	Investigando <d>	Confirmado, Cerrado, En curso, Abierto, Investigando, Resuelto
Researching (Investigando)	Resuelto <d>	Cerrado, Abierto, Resuelto, Esperando respuesta de usuario final, Cerrado, Abierto

Flujo de transición de orden de cambio

La tabla siguiente muestra el flujo de transición de orden de cambio predefinido.

Estado actual	Transición predeterminada	Siguientes estados disponibles
Aprobación en curso	Aprobado <d>	Aprobado, Cancelado, Cerrado
Aprobado	Programado <d>	Cancelado, Cerrado, Implementación en curso, Programado
Revertido		Aprobación en curso, Cerrado, Abierto, RFC
Cancelada		Closed (Cerrado)
Cliente en espera		Cancelado, Cerrado, Implementación en curso, Rechazado, Programado, Verificación en el curso
Hold (En espera)		Cancelado, Cerrado, Implementación en curso, Programado
Implementación en curso		Revertido, Cancelado, Cerrado, Cliente en espera, Rechazado, Programado, Distribuidor en espera, Verificación en curso
Open (Abierto)	RFC <d>	Aprobación en curso, Cancelado, Cerrado, Cliente en espera, Implementación en curso, Rechazado, RFC, Programado, Distribuidor en espera
Rechazado	Cerrado <d>	Aprobación en curso, Cancelado, Cerrado
RFC	Aprobación en curso <d>	Aprobación en curso, Cancelado, Cerrado, Cliente en espera, Implementación en curso, Abierto, Rechazado, Programado, Distribuidor en espera

Estado actual	Transición predeterminada	Siguientes estados disponibles
Programado	Implementación en curso <d>	Cancelado, Cerrado, Cliente en espera, Implementación en curso, Distribuidor en espera, Verificación en curso, Cancelado, Cerrado, Implementación en curso, Programado, Revertido, Cerrado

Procedimiento recomendado: transiciones de estado predefinidas

Las transiciones de estado predefinidas incluidas en el producto están "activas" en una nueva instalación e "inactivas" después de la actualización. Por cada estado que figura en la página de lista de transiciones, hay una transición de estado predeterminada (o estado siguiente). La ruta que toma la transición de estado predeterminada refleja el procedimiento recomendado. Las transiciones de estado adicionales que figuran en la página de lista de transiciones se proporcionan para satisfacer diversos workflows de gestión de tickets. Sin embargo, sólo las transiciones de estado "activas" que utilizan este procedimiento recomendado pueden garantizar que se produzca el workflow adecuado para gestionar solicitudes, incidentes, problemas y órdenes de cambio. Este procedimiento recomendado ayuda a promover el movimiento de tickets para la resolución y el cierre dentro del entorno de TI.

Por ejemplo, las siguientes transiciones predefinidas de incidente que figuran en la página Lista de transiciones de incidente se establecen como inactivas para ayudar a promover la resolución y el cierre de incidentes:

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.	Nuevo estado	Predeterminado	Status Description	Estado de registro
Acknowledged (Confirmado)	Closed (Cerrado)	No	Transición de estado de Confirmado a Cerrado	Inactivo

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.	Nuevo estado	Predeterminado	Status Description	Estado de registro
Acknowledged (Confirmado)	Cerrado y no resuelto	No	Transición de estado de Confirmado a Cerrar sin resolver	Inactivo
Acknowledged (Confirmado)	Open (Abierto)	Sí	Transición de estado de Confirmado a Abierto	Inactivo
Esperando respuesta de usuario final	Acknowledged (Confirmado)	No	Transmisión de estado de En espera de una respuesta del usuario final a Confirmado	Inactivo
Esperando respuesta de usuario final	Open (Abierto)	No	Transición de estado de Esperando respuesta de usuario final a Abierto	Inactivo
Esperando distribuidor	Acknowledged (Confirmado)	No	Transmisión de estado de Esperando distribuidor a Confirmado	Inactivo
Esperando distribuidor	Closed (Cerrado)	No	Transición de estado de Esperando distribuidor a Cerrado	Inactivo
Esperando distribuidor	Open (Abierto)	No	Transición de estado de Esperando distribuidor a Abierto	Inactivo
Closed (Cerrado)	Acknowledged (Confirmado)	No	Transición de estado de Cerrado a Confirmado	Inactivo
Cerrado y no resuelto	Acknowledged (Confirmado)	No	Transición de estado de Cerrado sin resolver a Confirmado	Inactivo
Cerrado y no resuelto	Closed (Cerrado)	No	Transición de estado de Cerrado sin resolver a Cerrado	Inactivo

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.	Nuevo estado	Predeterminado	Status Description	Estado de registro
Hold (En espera)	Acknowledged (Confirmado)	No	Transición de estado de En espera a Confirmado	Inactivo
Hold (En espera)	Closed (Cerrado)	No	Transición de estado de En espera a Cerrado	Inactivo
Hold (En espera)	Open (Abierto)	No	Transición de estado de En espera a Abierto	Inactivo
En curso	Acknowledged (Confirmado)	No	Transición de estado de En curso a Confirmado	Inactivo
En curso	Closed (Cerrado)	No	Transición de estado de En curso a Cerrado	Inactivo
En curso	Open (Abierto)	No	Transición de estado de En curso a Abierto	Inactivo
Open (Abierto)	Closed (Cerrado)	No	Transición de estado de Abierto a Cerrado	Inactivo
Pending Change (Pendiente de cambio)	Acknowledged (Confirmado)	No	Transición de estado de Cambio pendiente a Confirmado	Inactivo
Pending Change (Pendiente de cambio)	Closed (Cerrado)	No	Transición de estado de Cambio pendiente a Cerrado	Inactivo
Pending Change (Pendiente de cambio)	Open (Abierto)	No	Transición de estado de Cambio pendiente a Abierto	Inactivo

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.	Nuevo estado	Predeterminado	Status Description	Estado de registro
Researching (Investigando)	Open (Abierto)	No	Transición de estado de Investigación a Abierto	Inactivo

Transiciones de estado para el autoservicio

Las transiciones de estado le permiten controlar el movimiento de un ticket desde un estado discreto a otro (por ejemplo, de Abierto a Cerrado). Para los empleados que utilizan el autoservicio, puede incluir botones en los formularios de detalles de incidentes y peticiones para representar alguna transición de estado (see page 323).

Los botones de transición de estado para workflows de procesos de peticiones e incidentes aparecen en la interfaz del empleado cuando se vinculan transiciones de petición o incidentes con los tipos de transición activos. Los tipos de transición definen el texto de botón y controlan el comportamiento del formulario de detalles del ticket. Cuando se definen botones, los botones heredados Cerrar incidente (o solicitud) y Volver a abrir incidente (o solicitud) no se muestran en los formularios de detalles del ticket. En cambio, el empleado sólo puede cambiar el estado del incidente o solicitud mediante los botones de transición de estado configurados por el administrador.

De forma predeterminada, todos los tipos de transición predefinidos que se incluyen en el producto están inactivos, de modo que los botones de transición de estado no están activos. Como administrador del sistema, puede activar y modificar los tipos de transición predefinidos o crear tipos de transición para alojar sus workflows de transición de estado. Después de que cree o modifique un tipo de transición, lo puede vincular a cualquier transición de estado de petición o incidente.

Nota: Para obtener más información acerca de los tipos de transición, consulte la *Ayuda en línea*.

Más información:

[Cómo funcionan las transiciones para autoservicio](#) (en la página 337)

[Cómo crear o actualizar tipos de transición para transiciones](#) (en la página 338)

[Cómo vincular tipos de transición con transiciones](#) (en la página 338)

[Tipos de transiciones predefinidas](#) (en la página 339)

Cómo funcionan las transiciones para autoservicio

Los tipos de transición y sus estados correspondientes controlan cuándo los empleados pueden cerrar y volver a abrir los tickets de la siguiente manera:

1. El administrador vincula los tipos de transición activos con las transiciones de estado de petición o incidente.
2. El empleado crea un incidente mediante autoservicio.
3. El analista asignado al incidente encuentra una solución y mueve el ticket al estado Resuelto.
4. Cuando el ticket está en un estado Resuelto, el formulario de detalles del empleado muestra botones de transición de estado para aceptar o rechazar la resolución.
 - Si el empleado acepta la resolución, se produce la transición de Resuelto a Cerrado.
 - Si el empleado rechaza la resolución, se produce la transición de Resuelto a Abierto.
5. Después de que el empleado hace clic en un botón, puede agregar sus comentarios en el formulario de resolución que aparece.

Cómo crear o actualizar tipos de transición para transiciones

Como administrador del sistema, puede crear nuevos tipos de transición o actualizar tipos de transición existentes para flujos de trabajo de transiciones de estado de petición e incidente en la página Lista de tipos de transiciones.

Para crear un tipo de transición para una transición de estado, realice lo siguiente:

1. En la ficha Administración, seleccione Service Desk, Solicitudes/incidentes/problemas, Tipos de transición.
2. Haga clic en Crear en la página de la lista.
3. Edite los campos como sea apropiado en la página de detalles.
Se crea el tipo de transición para la transición de estado.
4. Haga clic en Guardar.

El nuevo tipo de transición aparece en la lista de tipos de transiciones cuando vuelve a visualizar la página.

Para actualizar un tipo de transición, realice lo siguiente:

1. Abra el tipo de transición deseado para editarlo en la página Lista de tipos de transiciones.
2. Edite los campos según sea necesario.
3. Haga clic en Guardar.

El tipo de transición actualizado aparece en la Lista de tipos de transiciones.

Cómo vincular tipos de transición con transiciones

Cuando se relacionan transiciones de estado con tipos de transición, el formulario de detalles del ticket del empleado muestra botones de transición de estado para aceptar o rechazar la resolución. Para vincular un tipo de transición con una transición de estado, realice lo siguiente:

1. En la ficha Administración, seleccione Service Desk, Peticiones/incidentes/problemas, Transiciones de incidente (o petición).
2. Abra la transición de estado deseada para editarla en la página Lista de transiciones de petición o incidente.
3. Especifique el tipo de transición deseado en el campo Tipo de transición.
4. Haga clic en Guardar.

El tipo de transición se vincula con la transición de estado.

Tipos de transiciones predefinidas

De forma predeterminada, todos los tipos de transición de muestra que se incluyen en el producto están inactivos, de modo que los botones de transición de estado no están activos. Es posible activar y modificar estos tipos de transición para que se ajusten al flujo de transición de estado deseado.

Para activar un tipo de transición predefinido, realice lo siguiente:

1. Seleccione Mostrar filtro en la página Lista de tipos de transiciones.
La parte superior de la página muestra más campos de búsqueda.
2. Seleccione Inactivo en el campo Estado del registro y, a continuación, haga clic en Buscar.
La Lista de tipos de transiciones muestra todos los tipos de transición inactivos.
3. Haga clic con el botón derecho del ratón en el tipo de transición deseado y seleccione Editar en el menú.
4. Seleccione Activo en el campo Estado del registro.
5. Haga clic en Guardar, Cerrar ventana.
6. Haga clic en Buscar.
La Lista de tipos de transiciones muestra el tipo de transición activo.

Más información:

[Tipos de transición de muestra para transiciones de estado de incidente](#) (en la página 339)

[Tipos de transición de muestra para transiciones de estado de solicitud](#) (en la página 340)

Tipos de transición de muestra para transiciones de estado de incidente

La siguiente tabla describe los tipos de transición de muestra para transiciones de estado de incidente:

Símbolo	Texto del botón	Texto del encabezado del formulario	Transición de estado de incidente
Botón Aceptar resolución de incidente	Aceptar	Aceptar resolución	Resuelto a Cerrado
Botón Rechazar resolución de incidente	Rechazar	Rechazar resolución	Resuelto a Abierto
Botón Rechazar	Solicitar el cierre	Solicitar el cierre	■ Abierto a Cerrado sin

Símbolo	Texto del botón	Texto del encabezado del formulario	Transición de estado de incidente
incidente de cierre			resolver ■ Esperando respuesta de usuario final ■ Esperando distribuidor ■ En curso ■ Acknowledged (Confirmado)

Tipos de transición de muestra para transiciones de estado de solicitud

La siguiente tabla describe los tipos de transición de muestra para transiciones de estado de solicitud:

Nota: El estado Petición de cierre para solicitudes es el equivalente del estado Resuelto para incidentes.

Símbolo	Texto del botón	Texto del encabezado del formulario	Transición de estado de solicitud
Botón Aceptar resolución de solicitud	Aceptar	Aceptar resolución	Petición de cierre a Cerrado
Botón Rechazar resolución de solicitud	Rechazar	Rechazar resolución	Petición de cierre a Abierto
Botón de solicitud de solicitud de cierre	Solicitar el cierre	Solicitar el cierre	■ Abierto a Cancelado ■ Esperando respuesta de usuario final ■ Esperando distribuidor ■ Aprobación en curso ■ Acknowledged (Confirmado)
Botón Cerrar solicitud	Cerrar	Cierre solicitado	De En curso a Cerrado

Temporizadores

Los temporizadores actúan como cronómetros que disponen de diversos umbrales y que indican a los analistas el tiempo transcurrido. Se puede definir la cantidad de tiempo que los temporizadores permanecen en los umbrales pero, además, existen opciones para que cambien de color, emitan pitidos o muestren recordatorios al llegar a cada umbral. Los analistas del servicio de asistencia no ejercen control alguno sobre el cronómetro, tan sólo el administrador.

Las solicitudes son el único tipo de ticket que emplea temporizadores, por lo tanto, éstos se deben configurar para los modelos de servicio de asistencia interno y combinado.

Éstos son los valores de los umbrales predefinidos de los temporizadores:

Duración de umbral	Color
00:00:00	Verde
00:01:00	Amarillo
00:05:00	Rojo

Con los valores predefinidos, los temporizadores son de color verde cuando se inician. Después de un minuto, cambian a amarillo y, después de cinco minutos, a rojo. El tiempo transcurrido se muestra cuando los analistas ven las solicitudes en detalle y se restablece cada vez que se selecciona otra solicitud. Es posible agregar pasos a este proceso o cambiar los existentes.

Los temporizadores se pueden marcar como activos o inactivos. Al marcarlos como inactivos, dejan de formar parte del proceso pero siguen guardados para su futuro uso, es decir, no se eliminan de las bases de datos. Si más tarde decide utilizar el temporizador, regrese a él y actívelo.

Zonas horarias

Puede configurar zonas horarias específicas para servidores, tipos de servicio, contactos y ubicaciones del sistema CA Service Desk Manager. Puede configurar tipos de servicio locales que se apliquen a una zona horaria específica y tipos de servicio globales que se apliquen a toda la empresa. De este modo, ya no es necesario que el administrador conozca la zona horaria de un servidor y ajuste manualmente las horas de los turnos de trabajo para que se adapten a diferentes zonas horarias.

Más información:

[Desencadenantes de eventos de tipo de servicio](#) (en la página 342)

[Cómo se utiliza una zona horaria](#) (en la página 343)

[Cómo determinar la zona horaria que se va a utilizar](#) (en la página 343)

Desencadenantes de eventos de tipo de servicio

Los tipos de servicio definen los eventos que se desencadenan después de cumplirse un retraso especificado.

Ejemplo: Desencadenantes de eventos por programación de turno

En este ejemplo, una programación de turno asociada con el tipo de servicio restringe el momento real en el que se desencadena un evento, de la siguiente manera:

- El turno de trabajo es de 8:00 a.m. a 5:00 p.m.
- El retraso del evento es de tres horas.
- La hora actual del servidor es 3:00 p.m.

El evento se desencadenará mañana a las 9:00 a.m. (hora del servidor) a causa de los siguientes hechos:

- Según la hora actual del servidor, quedan dos horas del turno de hoy (según la hora actual son las 3:00 p.m. y el turno finaliza a las 5:00 p.m.).
- El retraso del evento es de tres horas. Dos horas de este retraso se emplean en el turno del día de hoy (de 3:00 p.m. a 5:00 p.m.). La otra hora de retraso se traslada al turno del día siguiente (de 8:00 a.m. a 9:00 a.m.).

Por consiguiente, el evento se inicia a las 9:00 a.m. del día siguiente.

Cómo se utiliza una zona horaria

Una zona horaria asociada al tipo de servicio puede limitar las horas de activación de eventos.

Ejemplo: desencadenantes de eventos por zona horaria

En este ejemplo, una zona horaria asociada con el tipo de servicio restringe el momento real en el que se desencadena un evento, de la siguiente manera:

- El turno de trabajo es de 8:00 a.m. a 5:00 p.m.
- El retraso del evento es de tres horas.
- La hora actual del servidor es 3:00 p.m.
- La hora actual de la zona horaria es 12:00 p.m.

El evento se desencadenará hoy a las 6:00 p.m. (hora del servidor) a causa de los siguientes hechos:

- Según la hora actual del servidor, quedan dos horas del turno de hoy (según la hora actual son las 3:00 p.m. y el turno finaliza a las 5:00 p.m.).
- Según la hora actual de la zona horaria, quedan cinco horas del turno de hoy (según la hora actual son las 12:00 p.m. y el turno finaliza a las 5:00 p.m.).
- El retraso de evento es de tres horas (de 12:00 p.m. a 3:00 p.m. según la hora de la zona horaria y de 3:00 p.m. a 6:00 p.m. según la hora del servidor).

Por consiguiente, el evento se inicia a las 6:00 p.m. (hora del servidor) o a las 3:00 p.m. (hora de la zona horaria).

Cómo determinar la zona horaria que se va a utilizar

Puede especificar una zona horaria para un servidor, una ubicación y un tipo de servicio. También puede indicarle a CA Service Desk Manager que utilice la zona horaria del usuario final afectado de un ticket. CA Service Desk Manager utiliza las reglas siguientes para determinar la zona horaria que activa un evento:

- **Zona horaria del usuario final afectado:** CA Service Desk Manager utiliza esta regla cuando se dan las condiciones siguientes:
 - La opción Utilizar zona horaria de usuario final está seleccionada.
 - Se ha especificado una zona horaria para el usuario final afectado del ticket.

- **Zona horaria de la ubicación del usuario final afectado:** CA Service Desk Manager utiliza esta regla cuando se dan las condiciones siguientes:
 - La opción Utilizar zona horaria de usuario final está seleccionada.
 - No se ha especificado una zona horaria para el usuario final afectado del ticket.
 - Se ha especificado una zona horaria para la ubicación del usuario final afectado.
- **Zona horaria del tipo de servicio:** CA Service Desk Manager utiliza esta regla cuando se dan las condiciones siguientes:
 - Se ha especificado una zona horaria para el tipo de servicio.
 - La opción Utilizar zona horaria de usuario final no está seleccionada.
- **Zona horaria del servidor:** CA Service Desk Manager utiliza esta regla cuando se dan las condiciones siguientes:
 - Se ha especificado una zona horaria para el servidor.
 - La opción Utilizar zona horaria de usuario final no está seleccionada.
 - No se ha especificado una zona horaria para el tipo de servicio.
- **No hay compatibilidad de zona horaria:** CA Service Desk Manager utiliza esta regla cuando se dan las condiciones siguientes:
 - No se ha especificado una zona horaria para el tipo de servicio.
 - La opción Utilizar zona horaria de usuario final no está seleccionada.
 - No existe ningún registro de servidor.

Adjuntos de archivos

Con frecuencia, es necesario asociar un archivo con un ticket; en los ejemplos se incluyen los archivos siguientes:

- Una captura de pantalla de un error particular.
- Los archivos de registro que dan lugar a un problema.
- Un correo electrónico que explica un problema.
- Un vínculo que señala a una página Web que precisa una reparación.

Configure Service Desk de forma que los usuarios puedan trabajar con adjuntos. Todos los tipos de tickets se pueden acompañar de adjuntos, por lo tanto, configure adjuntos para todos los modelos de servicio de asistencia.

CA Service Desk Manager clasifica los adjuntos de la siguiente manera:

- **Almacenados:** los adjuntos almacenados se cargan y guardan en repositorios. Cuando los analistas revisan los adjuntos almacenados, éstos se recuperan con un explorador Web y se visualizan en el equipo local. El archivo almacenado permanece en el repositorio.

Los adjuntos almacenados se pueden cargar en los repositorios mediante servidores Web que empleen el protocolo HTTP. El uso de estos servidores con el fin de almacenar archivos permite el almacenamiento y la recuperación desde la interfaz de usuario. A los repositorios de unidades compartidas no se accede con eficacia desde los clientes Web, por lo que no se admiten.

- **Vinculado:** sólo almacena un vínculo al archivo de la base de datos.

Más información:

[Carga y descarga de archivos adjuntos](#) (en la página 345)

[Repositorios](#) (en la página 346)

Carga y descarga de archivos adjuntos

Todas las interfaces de cliente pueden acceder a los repositorios existentes para la carga y la descarga de archivos adjuntos con las siguientes excepciones:

- Sólo se puede acceder a los repositorios de archivos compartidos si el daemon del repositorio se ejecuta en un equipo con acceso a los archivos compartidos. El servidor del registro de repositorio (formulario de detalles) debe ser un equipo con Windows que disfrute de acceso a los elementos compartidos. Además, en el equipo también se debe ejecutar el daemon del repositorio de CA Service Desk Manager.

Nota: No se admiten repositorios de unidades compartidas en WIN2003.

- La descarga de archivos comprimidos se basa en el momento en el que se hayan cargado. Los adjuntos de versiones anteriores se descargan sin descomprimir. Descomprima el archivo en el equipo cliente; de lo contrario, los adjuntos cargados desde una interfaz de cliente también se descargarán sin descomprimir, es decir, el servidor descomprime los archivos antes de devolverlos durante la solicitud de descarga del cliente.

Nota: Los clientes heredados continúan funcionando del mismo modo y disponen de acceso inmediato a las nuevas cargas realizadas en los repositorios existentes.

Nota: Para obtener información sobre cómo trabajar con adjuntos, consulte la *Ayuda en línea*.

Repositorios

Los repositorios representan directorios de discos ubicados en equipos locales o remotos. Es posible disponer de un repositorio de gran tamaño o bien de varios pequeños. El modo en el que se estructuran los repositorios depende por completo de las prácticas y las necesidades empresariales.

Mover o combinar repositorios es sencillo porque todos los atributos relativos a los repositorios se definen en el registro del repositorio. Sólo se asocian a los partes el repositorio y el nombre del archivo oportunos.

Los archivos que se cargan en los repositorios permanecen en ellos. Cuando se solicita un archivo, se produce una de las acciones siguientes:

- Un explorador Web (HTTP) recupera y presenta una copia del archivo al usuario.
- La aplicación asociada a la extensión del archivo abre el archivo automáticamente.

Ejemplo: Cambio de la estructura de directorios de un servidor Web

Este ejemplo muestra cómo cambiar la estructura de directorios de un servidor Web

Cambie el valor de Cargar ruta del registro del repositorio.

Todos los adjuntos existentes señalan correctamente a la ubicación nueva de forma automática.

Configuración de repositorios

Para que los usuarios de CA Service Desk Manager puedan trabajar con adjuntos, hay que configurar los repositorios.

La arquitectura distribuida permite que un sitio configure sus repositorios según sus necesidades. El servlet de un repositorio no tiene que residir en el mismo servidor que los archivos adjuntos. Los sitios pueden tener un servlet central para acceder a todos los repositorios distribuidos o un servlet dedicado para cada uno de los servidores de repositorio.

Cuando configure los repositorios, considere las instalaciones siguientes:

- **Servidor de repositorio en un servidor de CA Service Desk Manager:** los sitios que designan un servidor de repositorio en un servidor de CA Service Desk Manager protegido (normalmente, un servidor secundario protegido por un cortafuegos) no necesitan exponer el servlet de dicho equipo. Por el contrario, se puede especificar un servlet que se ejecute en el servidor principal u otro servidor de CA Service Desk Manager sin restricciones y seguir cargando y descargando archivos en ese servidor sin problemas. Según la red que una los dos servidores de CA Service Desk Manager, se puede producir algún impacto en el rendimiento de la carga y la descarga.

Nota: Una buena manera de configurar un repositorio remoto es instalar un servidor secundario con el repositorio en el servidor remoto y establecer la ruta de carga en una ruta local.

- **Servlet en el mismo servidor que el servidor de repositorio:** los sitios que desean un rendimiento óptimo para la carga y descarga de adjuntos, y si el rendimiento de la red es un problema y se van a adjuntar archivos muy grandes, deberían considerar esta configuración. Esta configuración exige la exposición del puerto de Tomcat (por lo general, el 8080) en el servidor, lo cual es preciso tener en consideración si el equipo está protegido por un cortafuegos.

Requisitos del sistema

De forma predeterminada, los repositorios se ubican en el servidor primario, por lo que no hace falta ninguna tarea de configuración adicional para cargar los adjuntos de archivo. Sin embargo, si el repositorio está en un equipo remoto, hay que instalar un servidor secundario con rep_daemon ejecutándose en el servidor primario. Los requisitos del sistema del servidor son los siguientes:

- Servidor secundario (remoto) donde se ejecute el demonio del repositorio
- Servlet de carga y Tomcat

Procedimiento para configurar un repositorio en un equipo remoto

1. Abra un símbolo del sistema e introduzca:

```
cd $NX_ROOT/samples/pdmconf
```
2. Ejecute pdm_edit.pl.
Se le harán dos preguntas. Responda a ellas para volver al menú principal.
3. Seleccione 8 y pulse la tecla Intro para seleccionar Repository Daemon.

4. Escriba el nombre del servidor secundario y pulse la tecla Intro.

Nota: El nombre del servidor secundario debe coincidir con el valor NX_LOCAL_HOST del servidor secundario.

Aparece el menú principal.

5. Seleccione X y pulse Intro para guardar y salir.

El archivo guardado es el archivo pdm_startup.rmt, que reemplaza al archivo \$NX_ROOT/pdmconf/pdm_startup.tpl.

6. Cambie el nombre del archivo pdmconf/pdm_startup.tpl actual.

7. Copie el nuevo archivo pdm_startup.rmt en pdmconf/pdm_startup.tpl.

8. Instale el servidor secundario e inicie el supervisor en él.

Nota: En los sistemas Windows NT, el supervisor es un servicio y en Linux es pdm_proctor_nxd.

9. Inicie el servidor primario y utilice pdm_status para comprobar si aparece el nuevo daemon.

10. Cambie el nombre del servidor y la ruta de carga para que señale al equipo remoto donde se ejecuta el daemon del repositorio.

El equipo remoto está configurado para cargar los adjuntos de archivos.

Definición de repositorios

A continuación, debe definir un repositorio con la función administrativa de CA Service Desk Manager de la interfaz Web para utilizar archivos adjuntos.

Procedimiento para definir repositorios

1. Seleccione Adjuntos > Repositorio en el menú Administración para que se abra la página Lista de repositorios.

2. Seleccionar Archivo, Nuevo.

Aparecerá la página Detalles del repositorio.

3. Rellene los siguientes campos:

Símbolo

Identifica el repositorio con un nombre descriptivo: Sólo archivos grandes, Archivos permanentes, etc.

Repositorio predeterminado

Selecciona el repositorio automáticamente para todos los adjuntos. Los usuarios tienen la opción de cambiar a un repositorio distinto si lo desean.

Nombre de servidor

Especifica el nombre del servidor del repositorio.

Haga clic en Guardar.

4. Haga clic en OK.

Se cerrará la página de lista y de detalles y aparecerá la página principal.

Anuncios

Puede utilizar CA Service Desk Manager para enviar anuncios a los usuarios. Los anuncios ayudan a disminuir el número de llamadas entrantes y promueve una mayor productividad, gracias a la resolución proactiva de tickets y la comunicación de información importante a todos los usuarios afectados. Los usuarios se pueden desplazar por los distintos anuncios almacenados.

Nota: Los anuncios se aplican a todos los modelos de centro de servicio al usuario.

Se pueden agregar anuncios así como actualizar los existentes. Los anuncios forman parte de la función de datos de referencia de CA Service Desk Manager, de modo que puede utilizar el tipo de acceso para controlar los contactos que pueden crear anuncios.

Un anuncio puede especificar uno o los dos elementos que se describen a continuación:

Ubicación

Especifica una ubicación física, por ejemplo, una ciudad, edificio o piso.

Organization

Especifica un ID de organización. Cuando se establece Organización en un anuncio, solamente los individuos asignados a esa organización pueden ver el anuncio.

Cuando se establece Ubicación u Organización en un anuncio, solamente los contactos de esa ubicación u organización lo reciben. Cualquier contacto puede ver todos los anuncios que no se encuentran limitados por ubicación u organización. Por ejemplo, si no se establece ninguna de estas dos opciones, los contactos de todas las ubicaciones y organizaciones pueden ver un anuncio.

Nota: Los anuncios se especifican mediante la función administrativa de la interfaz Web. Para obtener más información sobre cómo definir los anuncios, consulte la *ayuda en línea*.

Más información:

[Visibilidad interna del anuncio](#) (en la página 350)

[Especificación de la urgencia del anuncio](#) (en la página 350)

Visibilidad interna del anuncio

Se puede controlar si un anuncio va a ser visible para los usuarios internos mediante la casilla de verificación Interno de la página Crear nuevo anuncio. El ajuste Ver registros internos del tipo de acceso del usuario conectado controla si un usuario puede ver elementos marcados como internos.

Especificación de la urgencia del anuncio

Puede especificar la urgencia de un registro de anuncio.

Procedimiento para especificar la urgencia del anuncio

1. Cree un anuncio o desplácese a la página Detalles de anuncio para editar un anuncio existente.
2. Seleccione uno de los valores siguientes en la lista desplegable Tipo de anuncio:

RUTINA

Aparece en texto negro.

ASESOR

Aparece en texto naranja.

Emergency

Aparece en texto rojo.

Haga clic en Guardar.

El registro de anuncio se identifica mediante colores en la página Lista de anuncios.

Configuración de consultas almacenadas

CA Service Desk Manager admite el uso de consultas almacenadas para generar dos tipos de datos:

- Las consultas del panel de resultados permiten personalizar el panel de resultados de la interfaz Web agregando campos de contador para los elementos de interés.
- Las consultas de KPI permiten recuperar información histórica de un período de tiempo especificado en el valor de un contador para utilizarla en la generación de informes basados en Web.

Las consultas almacenadas son aplicables a todos los modelos de servicio de asistencia; el propósito de las consultas almacenadas no consiste en llevar a los usuarios a otras páginas.

Los administradores definen las consultas almacenadas que estarán disponibles para los usuarios. Puede usar las consultas almacenadas predefinidas que se instalan junto con CA Service Desk Manager o definir otras propias. Puede definir las consultas almacenadas mediante la función administrativa de la interfaz Web.

Considere la información siguiente sobre las definiciones de consulta almacenadas:

- Las cláusulas de consultas almacenadas válidas están integradas en las instrucciones SELECT apropiadas y se introducen en el motor DBMS subyacente para su procesamiento. Para desarrollar las instrucciones SELECT, consulte los archivos de definición de objetos de los siguientes directorios:
 - Windows: directorio directorio-instalación\bopcfg:majic
 - UNIX: directorio \$NX_ROOT/bopcfg:majic
- Las consultas almacenadas emplean las instrucciones de atributos y objetos para crear las cláusulas WHERE de SQL en lugar de los nombres de campos de las bases de datos.
- CA Service Desk Manager no admite las uniones de productos cartesianos en las consultas almacenadas. Para garantizar que las consultas almacenadas no produzcan ninguna unión de productos cartesianos, escriba el siguiente comando adecuado según el sistema.
 - Windows: bop_cmd -f *directorio-instalación\bopcfg\interp\bop_diag.frg* "check_queries()"
 - UNIX: bop_cmd -f \$NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"

Actualice todas las consultas marcadas como resultado para impedir la aparición de uniones de productos cartesianos.

- Durante la creación de consultas almacenadas, se ofrece la opción de las consultas almacenadas de direcciones URL. Estas últimas ejecutan una consulta y devuelven resultados numéricos que sólo funcionan con Gestión del conocimiento.

Nota: Para obtener más información sobre la sintaxis de definición de objetos, consulte la *Guía de referencia técnica*. Para obtener más información acerca de cómo definir consultas almacenadas, consulte la *Ayuda en línea*.

Números de secuencias

Cuando se abre un parte, se le asigna automáticamente el siguiente número de secuencia disponible. Por ejemplo, si la última solicitud abierta tiene el número 5, a la siguiente se le asigna el número 6.

Importante: después de instalar una nueva versión de CA Service Desk Manager, el ID de registro interno de todos los tickets se restablece a 1. Para garantizar que no se creen ID de registro duplicados, no cree tickets nuevos antes de restaurar las copias de seguridad de los datos.

Para personalizar la numeración de las solicitudes, las órdenes de cambios y las incidencias, es necesario incluir un prefijo o sufijo exclusivo en el esquema de numeración. Por ejemplo, si desea realizar un seguimiento de las solicitudes por meses, agregue un identificador de mes como prefijo o sufijo al esquema de numeración de las solicitudes.

Nota: Para obtener información sobre cómo personalizar los números asignados a tickets con la función administrativa de la interfaz Web, consulte la *Ayuda en línea*.

Como se definen esquemas de numeración independientes para cada tipo de ticket, se deben configurar para todos los modelos de servicio de asistencia. Puede controlar el formato de la numeración de solicitudes, órdenes de cambio e incidencias cambiando los valores de los números de secuencia. De forma predeterminada, los partes nuevos se numeran con números enteros consecutivos. Como el campo de número de los tickets es en realidad un campo de cadena y no numérico, se asignan valores de cadena adicionales como prefijos o sufijos que se generan para los tickets nuevos. Por ejemplo, se pueden especificar r:, c:, e i: como prefijos de solicitudes, órdenes de cambio e incidentes. Esta configuración permite que los usuarios diferencien fácilmente entre los diversos tipos de ticket y eviten la confusión.

En los sistemas configurados para ITIL, los incidentes y los problemas comparten los esquemas de numeración con las solicitudes, porque los incidentes y los problemas son tipos de solicitudes diferentes desde el punto de vista interno.

Uso de registros de auditoría

CA Service Desk Manager crea un registro de auditoría que registra la información siguiente:

- Todos los cambios de una incidencia (Issue)
- Todos los cambios de una solicitud (Call_Req)
- Todos los cambios de una orden de cambio (Change_Request)
- Todos los cambios de una tabla de partición de datos (Domain)
- El ID de inicio de sesión de la persona asociada con el cambio y el sello de día/fecha/hora asociado
- Los valores previos y posteriores de la actualización, inserción o eliminación
- La creación de contactos
- (Configuración de ITIL) Actividades de creación y actualización del objeto

Nota: El registro de auditoría captura las modificaciones sólo del campo de partición de datos del contacto, pero ninguna otra actualización del registro de contacto.

La función Registro de auditoría se instala automáticamente, pero para activarla el usuario debe instalar dos opciones de registro de auditoría con el Gestor de opciones: audit_ins y audit_upd. Después de haber instalado estas opciones, puede acceder al registro de auditoría desde la ficha Administración seleccionando Service Desk, Lista de registros de auditoría. Puede buscar la lista de registros de auditoría con una herramienta de búsqueda integrada para que sea más fácil generar informes.

Nota: Para obtener más información sobre cómo instalar y establecer valores para las opciones, consulte la *ayuda en línea*.

Integración con CA Network and Systems Management

Es posible definir registros de mensajes de gestión de eventos así como acciones de registros de mensajes asociadas en CA NSM con el fin de crear solicitudes, adjuntar comentarios a las solicitudes existentes o enviar anuncios a CA Service Desk Manager automáticamente.

Nota: Para obtener más información sobre la integración con CA NSM, consulte la *Guía de implementación*.

Capítulo 8: Control del comportamiento del sistema

Esta sección contiene los siguientes temas:

[Uso del Gestor de opciones](#) (en la página 355)

[Cómo modificar el entorno del sistema](#) (en la página 356)

[Eventos](#) (en la página 357)

[Macros](#) (en la página 357)

Uso del Gestor de opciones

El cliente Web de CA Service Desk Manager le permite utilizar el Gestor de opciones desde la ficha Administración para hacer lo siguiente:

- Establecer opciones
- Obtener una lista de todas las opciones disponibles
- Ver un resumen de las opciones que revela, por ejemplo, la aplicación a la que están asociadas, su descripción o su estado.
- Ver los detalles de cualquier opción

Mientras se consultan los detalles de cualquier opción, se puede ver una descripción completa de sus funciones en la *ayuda en línea*. En la *ayuda en línea* se incluyen las acciones especiales que se deben llevar a cabo al modificar la opción. Por ejemplo, cuando se instalan o desinstalan algunas opciones, es preciso reiniciar el servidor de CA Service Desk Manager para que los nuevos valores de la opción surtan efecto. Si es el caso, se indica en la descripción correspondiente a la opción de la *ayuda en línea*.

- Revisar el estado de todas las opciones en los resúmenes
- Desinstalar cualquiera de las opciones disponibles

Muchas de las opciones se preconfiguran e instalan durante la instalación de CA Service Desk Manager. Utilizar el Gestor de opciones para instalar o desinstalar opciones puede alterar algunas o todas las opciones de configuración predeterminadas.

- Instalar cualquier opción definida

Nota: Durante el cambio de versiones, el servicio de asistencia técnica de CA Service Desk Manager puede poner a disposición del usuario opciones en respuesta a las solicitudes de los usuarios. Si desea obtener más información sobre estas opciones, póngase en contacto con el servicio técnico de CA Service Desk Manager. Para obtener más información sobre cómo utilizar el Gestor de opciones, consulte la *ayuda en línea*.

Cómo modificar el entorno del sistema

CA Service Desk Manager utiliza las variables de entorno especificadas en el archivo de plantillas de entorno (NX.env.tpl) para determinar ciertos comportamientos. Puede utilizar las variables de entorno para modificar ciertos comportamientos de sistema. Normalmente, se utiliza el gestor de opciones para controlar el comportamiento del sistema, pero a veces el Soporte técnico de CA le puede indicar que modifique directamente una variable del entorno concreta.

A la hora de editar el archivo de plantillas de entorno, tenga en cuenta lo siguiente:

- Las variables de entorno definidas en este archivo se pueden anular definiéndolas en el espacio de procesos donde éstos se ejecutan. Aunque es conveniente en algunos casos limitados, esta configuración normalmente no resulta deseable. Si se precede una configuración de variable con un símbolo de arroba (@), se evita que las variables del espacio de proceso sustituyan la variable. A menos que haya un motivo específico para permitir una sustitución, el símbolo @ siempre debe preceder al nombre de la variable en el archivo de plantillas.
- Los caracteres de comentario para este archivo son el signo numeral (#) y el signo de exclamación de cierre (!). El signo de exclamación de cierre también se utiliza para deshabilitar una opción.

Importante: modifique el archivo de plantillas (NX.env.tpl) y permita que el proceso de configuración aplique los cambios en el archivo de entorno. Nunca modifique el archivo de entorno (NX.env) directamente, ya sea en las instalaciones del servidor secundario o cliente.

Procedimiento para modificar el archivo de plantillas de entorno

1. Realice una copia de seguridad del archivo de plantillas de entorno (.tpl) correspondiente al entorno del sistema:
 - UNIX: \$NX_ROOT/pdmconf/NX.env.tpl.
 - Windows: installation-directory\pdmconf\NX.env_nt.tpl.
2. Edite el archivo de plantillas de entorno en el servidor primario. Este archivo se visualiza y modifica con cualquier editor de texto (en Windows, se utiliza WordPad).

3. Realice los cambios tal como lo indica el técnico de soporte y guarde los cambios.
4. Ejecute la función de configuración en la instalación del servidor principal para aplicar los cambios realizados en el archivo de plantillas de entorno al archivo de entorno existente.

Nota: Para obtener información sobre cómo ejecutar la utilidad de configuración, consulte la *Guía de implementación*.

5. Detenga y reinicie el servidor principal de CA Service Desk Manager para que se apliquen los cambios realizados en el archivo de entorno. Para evitar el apagado total del sistema, el técnico de soporte puede recomendarle que detenga y reinicie sólo determinados procesos en lugar de reiniciar todo el servidor de CA Service Desk Manager.

Eventos

Puede configurar eventos adjuntos a objetos para ejecutar acciones configuradas. Los eventos son procedimientos que se ejecutan después de que haya transcurrido una cantidad de tiempo determinada. Por ejemplo, un evento envía un mensaje a un analista de Service Desk si una incidencia de "prioridad 1" no se recibe en el plazo de una hora. Otras partes del sistema utilizan eventos, por ejemplo, tipos de servicio.

Puede definir eventos para solicitudes, incidentes, problemas, órdenes de cambio, incidencias, contactos, elementos de configuración y clientes globales y específicos. CA Service Desk Manager programa la hora de ejecución de los eventos en función del retraso y el turno.

Nota: Para obtener más información sobre los eventos, consulte la *Ayuda en línea*.

Macros

Las macros son pequeñas secuencias de comandos que definen condiciones o acciones. La ejecución de un evento o comportamiento puede implicar la ejecución de una o varias macros de acciones. Antes de que se ejecuten las macros, se puede utilizar una macro condicional para determinar el conjunto de macros de acciones que se ejecutarán.

Puede utilizar macros en las siguientes áreas:

- Eventos
- Plantillas de comportamientos de cambios o incidencias
- Notificaciones de actividades

El producto incluye varias macros. Los usuarios pueden crear tipos adicionales.

Nota: Aunque los clientes no pueden agregar macros de acciones o de condiciones, sí pueden crear condicionales simples con condiciones definidas por el sitio. Las condiciones definidas por el sitio son macros no complejas que se pueden crear en los cuadros de diálogo de la interfaz gráfica de usuario, pero que no sustituyen a las macros de condiciones.

Se debe especificar en cada macro el tipo de objeto que debe usar la macro. Por ejemplo, para crear una macro condicional definida por el sitio que compruebe los valores de las solicitudes, se debe establecer el tipo en la opción Solicitud. Al seleccionar las macros para los eventos y los comportamientos, CA Service Desk Manager sólo muestra las macros cuyo tipo coincide con el del evento o el comportamiento.

Tipos de macros

Cada una de las siguientes macros tiene un tipo específico que describe su uso:

Acción

Ejecuta algún tipo de acción como, por ejemplo, aumentar la prioridad de una incidencia.

Adjuntar evento

Adjunta un objeto de evento a un cambio, una incidencia, una solicitud, un contacto o un elemento de configuración.

Condición

Evalúa algunas macros condicionales verdaderas o falsas.

Ejecutar acción de CA IT PAM

Ejecuta una acción de CA IT PAM. CA IT PAM es un motor de workflow que habilita la gestión y la generación de informes en grupos de tareas que pueden requerir aprobaciones electrónicas.

Ejecutar acción de CA Workflow

Ejecuta una acción de CA Workflow. CA Workflow permite gestionar procesos de workflow en un entorno, como actividades de seguimiento que se completan en tickets asociados con una categoría o área específica.

Referencia remota

Inicia un programa externo en el servidor.

Notificación múltiple

Envía una notificación a uno o más contactos. Este tipo de macro resulta de especial utilidad, ya que permite especificar el mensaje, los destinatarios y el nivel de urgencia.

Condic. definida por el depto.

Crea eventos basados en condicionales verdaderas o falsas, según los atributos del ticket, para imponer niveles de servicio. Por ejemplo, puede crear una macro de condiciones que se evalúe como verdadera si las solicitudes son de prioridad 1, pero aún no se han asignado. Puede adjuntar la condición a un evento que se ejecute poco después de haber creado una solicitud.

Uso de macros con eventos

En el campo Condición de evento de Detalles de evento puede especificar una macro condicional, si así lo desea. Además, puede especificar la cantidad de macros que desee (que no sean condicionales) en las columnas de acciones verdaderas o falsas. Cada vez que se activan los eventos, se evalúa en primer lugar la macro condicional. Si se considera verdadera, se activan todas las macros de la columna de acciones en caso verdadero. Si se considera falsa, se activan todas las macros de la columna de acciones en caso falso. Además, las macros condicionales pueden comprobar si se han definido el asignatario, la prioridad, la infracción del tipo de servicio, etc. En caso de que no se especifique ninguna macro de condición de evento, éste ejecuta de forma automática las macros en caso verdadero.

En los detalles de los eventos, cabe la posibilidad de seleccionar casi cualquier tipo de macro con el fin de enviar notificaciones a los contactos, definir valores en los objetos de contexto, ejecutar referencias remotas o adjuntar otros eventos.

Uso de macros en el comportamiento de las categorías de cambios e incidencias

Las macros también se pueden utilizar en el comportamiento de las categorías de cambios e incidencias. En los detalles de las categorías, diríjase a la ficha Workflow y seleccione un estado. A continuación, en la ventana Detalles del workflow, haga clic en el botón Comportamiento. Entonces, de manera similar a los eventos, puede definir una condición y las acciones resultantes.

En la ficha Transición de los detalles del comportamiento se especifican las macros de tipo condicional para determinar si las tareas pueden salir del estado en el que se encuentren. Éstas se activan cuando el usuario intenta cambiar el estado de las tareas. Si la condición se considera falsa, se impide la actualización del estado.

Las tareas de workflow reales se crean a partir de las plantillas de la plantilla de la categoría. Cuando se cambia y guarda el valor de estado de las tareas, se activa el comportamiento especificado en la plantilla de la categoría, lo que significa que se ejecutan tanto la condición como las acciones resultantes.

Nota: Utilice una macro Adjuntar evento para adjuntar eventos a las tareas de workflow.

Uso de macros con Notificación múltiple

Notificación múltiple

El cuerpo del mensaje de la notificación múltiple señala directamente a la tabla del objeto seleccionado. Por lo tanto, al hacer referencia a los campos de la tabla de objetos, por ejemplo, CR (Call_Req), es posible hacer referencia al nombre del atributo del campo pertinente. Si desea especificar la información descriptiva del ticket de solicitud de llamada, puede escribir lo siguiente en el cuerpo del mensaje:

Descripción: @{description}

Una QREL (relación de consultas) es una relación que contiene una lista de objetos definidos por una cláusula WHERE de tipo SQL. Puede agregar la QREL a la descripción de una macro de notificación múltiple. Si desea colocar la QREL en la descripción de act_log QREL <-- alg, puede utilizar lo siguiente en una macro de notificación:

@{act_log.0.description}

Puede utilizar variables de reemplazo para hacer más relevantes y dinámicos los mensajes de notificación. Éstas adoptan la forma de @{ruta_atributo}, donde ruta_atributo es un atributo de algún objeto de CA Service Desk Manager. Al enviar la notificación, se reemplaza la variable por el valor de atributo especificado.

Las notificaciones (procedan de registros de actividades o de notificaciones múltiples) siempre cuentan con algún contexto base (un punto de referencia) que, en general, suele ser algún ticket o alguna tarea de workflow. En la notificación múltiple, el campo de tipo de macro de notificación especifica el objeto base. Puede utilizar la sintaxis @{} para hacer referencia a cualquier atributo del objeto.

Ejemplo: tenemos una notificación múltiple del tipo Solicitud que hace referencia a cualquier atributo del objeto cr (Call_Req). A fin de incluir la descripción de la solicitud, habría que especificar `@{description}`. La notación con puntos se usa para seguir las referencias a otros objetos. Por ejemplo, para incluir el apellido del asignatario de la solicitud: `@{assignee.last_name}`.

Uso de macros con una condición definida por el sitio

Condic. definida por el depto.

Las macros de condiciones están compuestas por al menos una condición *elemental*. Cada elemento prueba el valor de un solo atributo. Por lo tanto, si los usuarios desean definir la condición en función de los valores del asignatario y la categoría, es probable que la macro condicional deba emplear dos elementos, uno para el asignatario y otro para la categoría. Cuando estas macros se usan en eventos, los elementos se suelen conectar mediante operadores booleanos, sobre todo 'Y' u 'O'.

La ventana de detalles de macro condicional muestra una lista de elementos como la siguiente:

Atributo	Operador	Valor	Conector lógico	Traducción
Asignado	Igual	Jones	Y	El asignatario es Jones y...
Coste	Menor que	600	O	El coste es un valor entero menor que 600 o...
Group	Empty/NULL		Y	El campo Grupo está en blanco.

Nota: Los conectores lógicos (Y, O) conectan dos elementos. Cuando aparecen dos elementos como el uno y el dos, se conectan mediante el conector del elemento uno y se prescinde del conector del elemento dos. Es más, algunas selecciones de operadores no se emplean, por ejemplo, cuando uno de los atributos es *Asignatario* y aparece el operador *Menor que*; su uso no tendría sentido. Para obtener más información acerca de cómo crear macros condicionales, consulte la *Ayuda en línea*.

Capítulo 9: Configuración de la interfaz Web

Esta sección contiene los siguientes temas:

[Configuración de la interfaz Web](#) (en la página 363)
[Funcionamiento de la interfaz Web](#) (en la página 364)
[WebDirector y distribución de la carga Web](#) (en la página 364)
[WebDirector y configuración de motores Web](#) (en la página 369)
[Mejora del funcionamiento con el almacenamiento en caché de los exploradores](#) (en la página 400)
[Comportamiento de bloqueo de registros en la interfaz Web](#) (en la página 403)
[Impresión de páginas Web de CA Service Desk Manager](#) (en la página 404)
[Modificación del archivo de configuración](#) (en la página 404)

Configuración de la interfaz Web

La *interfaz Web* ofrece funciones de CA Service Desk Manager a través de Internet. La interfaz Web posibilita una navegación independiente de la base de conocimientos, reduciendo el número de llamadas al servicio de asistencia y acelerando los tiempos de resolución. La interfaz también le permite hacer lo siguiente:

- Abrir, procesar y cerrar tickets
- Visualizar y publicar anuncios
- Acceder a los datos de asistencia

Una vez que se ha instalado y configurado CA Service Desk Manager según las instrucciones de la *Guía de implementación*, puede administrar y proteger el uso de CA Service Desk Manager y configurarlo para adaptarlo a sus necesidades. La configuración de la seguridad de la interfaz Web se realiza mediante el uso de roles y tipos de acceso. Puede adaptar la interfaz para utilizarla con exploradores Web.

Funcionamiento de la interfaz Web

La interfaz Web de CA Service Desk Manager utiliza un servidor HTTP estándar como Tomcat, Apache o Microsoft Internet Information Server (IIS).

- Con el servidor Tomcat, un Java Servlet, el pdmweb.jar, procesa las solicitudes Web.
- Con Apache o el servidor IIS, una interfaz CGI, pdmweb.exe, procesa las solicitudes Web.

La interfaz Web de CA Service Desk Manager funciona de la siguiente manera:

1. Cuando los usuarios solicitan alguna página Web de CA Service Desk Manager, el servidor HTTP invoca pdmweb.jar o pdmweb.exe; de este modo, se configura una conexión al daemon de CA Service Desk Manager (o servicio de Windows) pertinente, que se denomina motor Web.
2. El motor Web interpreta entonces la solicitud del usuario. Casi todas las solicitudes exigen que el motor Web busque algún archivo de plantillas HTML (HTMPL) y lo convierta a código HTML estándar.
3. Por lo general, para el proceso de conversión es necesario que el motor Web se comuniquen con un servidor de CA Service Desk Manager a fin de leer o actualizar la base de datos e incluir información de la base de datos en el código HTML generado.
4. Una vez que se finaliza el código HTML, el motor Web lo envía a pdmweb.jar o a pdmweb.exe que, a su vez, lo vuelve a enviar al explorador del usuario.
5. Después de que los datos se han devuelto al explorador, finaliza el proceso de pdmweb.exe aunque el proceso de pdmweb.jar continúa activo.

WebDirector y distribución de la carga Web

A medida que aumenta el uso Web del departamento, puede resultar útil distribuir la carga entre varios motores Web, varios servidores HTTP o ambos. Esta distribución permite ampliar la capacidad del servidor Web con objeto de acomodar el uso que exige la organización. Puede utilizar WebDirector, suministrado con CA Service Desk Manager, para distribuir la carga Web. WebDirector recibe las solicitudes de conexión de los usuarios, selecciona el motor Web que se debe ocupar de ellas y las redirige a dicho motor. A excepción del cambio de dirección URL, se trata de un proceso que pasa inadvertido para el usuario final, que accede siempre a CA Service Desk Manager con la misma dirección URL independientemente del número de motores Web configurados.

Puede utilizar WebDirector de las siguientes formas:

- Para configurar CA Service Desk Manager para el uso eficaz de sockets seguros (SSL).

El protocolo HTTPS permite el cifrado de las transacciones Web y, de esta manera, ofrece la máxima seguridad a los datos confidenciales, en especial las contraseñas. No obstante, las páginas que usan SSL no son aptas para el almacenamiento en la caché del explorador, lo que ejerce un impacto negativo sobre el rendimiento.

- Para dirigir los inicios de sesión a un motor Web específico (o motores Web).

Tras la autenticación de los usuarios, WebDirector puede trasladar la sesión a otros motores Web que pueden estar ubicados en servidores HTTP distintos. Esta posibilidad permite configurar SSL para un motor Web de inicio de sesión concretos, lo que proporciona una máxima protección para las contraseñas, al tiempo que se reserva el protocolo HTTP estándar para las demás transacciones y, por tanto, se consigue el máximo rendimiento.

- Para tener varios WebDirector, cada uno ocupándose de un grupo diferente de motores Web.

Esto puede resultar de utilidad en organizaciones dispersas geográficamente que deseen disponer de grupos de motores Web situados en ubicaciones físicas más próximas a los usuarios finales.

Web.cfg y CA Service Desk Manager

La secuencia de comandos `pdm_edit.pl` que se suministra puede servir para facilitar la configuración de los motores Web de CA Service Desk Manager. Sin ella, los usuarios que agreguen motores Web deben especificar su nombre de forma manual y crear una instancia única del archivo `web.cfg`. El script hace estas tareas automáticamente.

Al usar la secuencia de comandos `pdm_edit.pl` para configurar algún motor Web, esta secuencia procede a la creación y la nominación automáticas de la secuencia apropiada. El nombre se elabora del modo siguiente:

`"<Nombre_Host>-web[nº].cfg"`

nombre de host

Especifica el servidor como primario cuando el motor Web reside en un servidor primario, o especifica el nombre de host de servidor real cuando el motor Web reside en un servidor secundario.

[nº]

Especifica un valor entero que asigna de forma automática la secuencia `pdm_edit.pl` y que aumenta en progresión por cada motor Web de los servidores.

La instalación de CA Service Desk Manager ofrece un archivo de configuración para el motor Web predeterminado que se define en esta ubicación:

`$NX_ROOT/bopcfg/www/web.cfg`

Una vez modificado el motor Web predeterminado mediante la secuencia `pdm_edit.pl`, el nombre del archivo de configuración correspondiente que se genera sigue este esquema de nombres:

`<Nombre_Host>-web[nº].cfg`

En lo sucesivo, se pasa por alto el archivo `web.cfg` original junto con las personalizaciones realizadas. Si el usuario desea conservar alguna de las personalizaciones del archivo `web.cfg` original, debe asegurarse de seleccionar `$NX_ROOT/bopcfg/www/web.cfg` como el archivo de plantilla que debe emplear la secuencia `pdm_edit.pl` al crear los archivos `<Nombre_Host>-web[nº].cfg`.

Asignación de motores Web a un WebDirector

Los motores Web se asignan a un WebDirector mediante los parámetros pertinentes del archivo de motores Web siguiente:

`'<Nombre_Host>-web[nº].cfg'`

Cabe destacar que, mientras que cada uno de los motores Web necesita su propio archivo `<Nombre_Host>-web[nº].cfg`, los WebDirector no emplean ningún archivo de configuración Web. La asignación de motor Web y WebDirector se realiza inicialmente mediante el script de esta utilidad:

`'pdm_edit.pl'`

Quizá sea preciso aplicar más cambios en los parámetros de WebDirector del archivo `<Nombre_Host>-web[nº].cfg` correspondiente al motor Web a fin de modificar el comportamiento de redirección del motor. Si no se asigna un motor Web a un WebDirector (opción predeterminada), el parámetro `'UseDirector'` del archivo de configuración del motor Web se establece en `'No'`. En ese caso, CA Service Desk Manager ignora los demás parámetros de `'Webdirector'` para el motor Web.

En cuanto se asigna un motor Web a un WebDirector, los parámetros siguientes definen la interacción entre ambos:

- `UseDirector` Yes | No | AfterLogin | BeforeLogin
- `WebdirectorSlumpName` (el nombre de slump se asigna de forma automática)

- WillingnessValue (de '0' a '10')
- RedirectingURL [http/https]://<nombredelequipo>/<directorio cgi>/<nombre cgi>

Definición del rol de los motores Web según los parámetros de WebDirector

Después de haber configurado un motor Web para que use un Web Director, dicho motor asume un rol distinto. Este rol define las solicitudes de los clientes Web de las que se debe ocupar el motor Web. Éstos son los posibles roles:

- Atención sólo de las solicitudes de inicio de sesión (redirige las restantes a otra parte)
- Atención sólo de las solicitudes que no sean de inicio de sesión (redirige las de inicio de sesión a otra parte)
- Atención tanto de las solicitudes de inicio de sesión como de las solicitudes restantes (motor Web para fines generales)

El rol está condicionado por los valores de los parámetros de 'WebDirector' que aparecen en el archivo '<Nombre_Host>-web[nº].cfg' del motor Web. En la tabla siguiente se ilustra la relación entre el rol de los motores Web y el valor de los parámetros de WebDirector:

Rol de motores Web	Valores de parámetros de 'webdirector' del archivo '<Nombre_Host>-web[nº].cfg'
Atención de solicitudes de inicio de sesión	'UseDirector AfterLogin'; 'Willingness 0'
Atención de actividades no relacionadas con el inicio de sesión	'UseDirector BeforeLogin'; 'Willingness [1-10]'
Fines generales	'UseDirector Yes'; Willingness [1-10]'

Entorno no SSL con equilibrio de carga básico

Puede utilizar WebDirector en un entorno no SSL con equilibrio de carga básico. WebDirector equilibra la carga entre todos los motores Web de acuerdo con el valor de disposición de cada motor. El motor Web pueden atender solicitudes de inicio de sesión y solicitudes que no estén relacionadas con el inicio de la sesión. El protocolo HTTP permite la comunicación entre los clientes Web y los servidores Web.

En todo motor Web que esté sometido al control de WebDirector, defina los parámetros pertinentes del archivo `<Nombre_Host>-web[nº].cfg` que corresponda al motor del modo siguiente:

- UseDirector Yes
- WebDirectorSlumpName (no cambie este valor)
- WillingnessValue [1-10]
- RedirectingURL (el valor del protocolo colocado delante puede faltar o ser "http")

Entorno SSL global con equilibrio de carga básico

Puede utilizar WebDirector en un entorno SSL global con equilibrio de carga básico. WebDirector equilibra la carga entre todos los motores Web de acuerdo con el valor de disposición de cada motor. Cada motor Web puede atender solicitudes de inicio de sesión y solicitudes que no estén relacionadas con el inicio de la sesión. Se emplea el protocolo HTTPS para la comunicación entre los clientes Web y los servidores Web.

En todo motor Web que esté sometido al control de WebDirector, defina los parámetros pertinentes del archivo `<Nombre_Host>-web[nº].cfg` que corresponda al motor del modo siguiente:

- UseDirector Yes
- WebDirectorSlumpName (no cambie este valor)
- WillingnessValue [1-10]
- RedirectingURL (el valor del protocolo colocado delante debe ser "https")

Inicio de sesión en entorno no SSL con equilibrio de carga opcional

Puede utilizar WebDirector para un inicio de sesión de destino en un entorno no SSL con equilibrio de carga opcional. El motor Web sólo de inicio de sesión atiende únicamente las solicitudes de inicio de sesión. Los restantes motores Web sometidos al control de WebDirector atienden las demás solicitudes. Esta configuración hace recaer toda la carga de la atención de las solicitudes de inicio de sesión en los motores Web especificados para el inicio de sesión exclusivamente. Se emplea el protocolo HTTP para la comunicación entre los clientes Web y los servidores Web.

En el caso de los motores Web exclusivos de inicio de sesión, defina los parámetros de WebDirector del archivo `<Nombre_Host>-web[nº].cfg` que corresponda al motor del modo siguiente:

- UseDirector AfterLogin
- WebDirectorSlumpName (no cambie este valor)
- WillingnessValue 0
- RedirectingURL (el valor del protocolo colocado delante puede faltar o ser "http")

En el caso de los motores Web ajenos al inicio de sesión, defina los parámetros de WebDirector del archivo `<Nombre_Host>-web[nº].cfg` que corresponda al motor del modo siguiente:

- UseDirector BeforeLogin
- WebDirectorSlumpName (no cambie este valor)
- WillingnessValue [1-10]
- RedirectingURL (el valor del protocolo colocado delante puede faltar o ser "http")

Inicio de sesión SSL en entorno mixto con equilibrio de carga opcional

Puede utilizar WebDirector para un inicio de sesión SSL en un entorno SSL mixto o en un entorno no SSL con equilibrio de carga opcional. Todas las solicitudes de inicio de sesión en Web se redirigen a los motores Web SSL, que se ocupan de atenderlas, mientras que las demás solicitudes se redirigen a los motores Web que no son SSL, que son los que las atienden. Se emplea el protocolo HTTPS para la comunicación entre los clientes Web y los motores Web SSL.

WebDirector y configuración de motores Web

Familiarícese con la siguiente información para agregar y configurar WebDirector y motores Web, basándose en los tipos de servidor y componente:

SSL

Especifica el protocolo de nivel de socket seguro.

pdm_edit.pl

Especifica el script Perl de CA Service Desk Manager que se emplea para agregar y modificar motores Web, WebDirector, gestores de objetos y otros componentes.

Interfaz CGI

Especifica el nombre de script de los motores Web y WebDirector asignados por pdm_edit.pl. Este valor es el nombre de una CGI real ejecutable cuando se utiliza IIS o Apache como servidor HTTP; es un parámetro de servlet cuando se utiliza Tomcat como servidor HTTP.

Por ejemplo: (motores Web) pdmweb1, pdmweb2, (WebDirector) pdmweb_d1 y pdmweb_d2

Los sistemas que utilizan servidores de servlet como Tomcat no necesitan ejecutables de interfaz CGI. La interfaz CGI se simula por medio de un servlet que se ejecuta en el servidor de servlet, en su lugar, estos sistemas deben disponer de un archivo web.xml en el directorio: \$NX_ROOT/bopcfg/CATALINA_BASE/webapps/CAisd/WEB-INF

Pdm_edit.pl crea archivos web.xml de ejemplo, cuyo nombre sigue la estructura *<nombrehost>-web.xml.tpl*. Copie estos archivos en el servidor apropiado del directorio WEB-INF para que sustituyan el archivo web.xml.tpl de cada servidor y vuelva a configurar el servidor secundario.

Inicio de sesión SSL

Especifica la configuración de CA Service Desk Manager en la que al menos uno de los motores Web reside en un directorio virtual con SSL impuesto y se ocupa en exclusiva de todas las solicitudes de inicio de sesión de los clientes Web mediante comunicaciones cifradas por HTTP. Una vez realizada la autenticación, un WebDirector redirige el cliente Web a otro motor Web apto que resida en un directorio virtual donde no se haya impuesto SSL para el resto de la sesión mediante comunicaciones no cifradas por HTTP.

Motor Web de inicio de sesión seguro

Especifica el motor Web del entorno de inicio de sesión SSL que se ocupa en exclusiva de todas las solicitudes de autenticación de los usuarios de los clientes Web de CA Service Desk Manager.

Motor Web no seguro

Especifica el motor Web del entorno de inicio de sesión SSL que se ocupan de todas las solicitudes que no se refieran a la autenticación de los usuarios de los clientes Web después de que se haya producido la autenticación en el motor Web de inicio de sesión seguro.

Rol de motores Web

Especifica las tareas que lleva a cabo el motor Web una vez que se han asignado a un WebDirector. Éstos son los posibles roles:

- Procesamiento sólo de las solicitudes de inicio de sesión de los clientes Web.
- Procesamiento de todo salvo de las solicitudes de inicio de sesión de los clientes Web.
- Procesamiento de todas las solicitudes de los clientes Web.

Cómo implementar un entorno de inicio de sesión SSL con un servidor primario solamente

Puede implementar un entorno de inicio de sesión SSL que utilice sólo un servidor primario.

Nota: Para crear este sistema, debe estar instalado y configurado el servidor primario.

Para implementar un entorno de inicio de sesión SSL, haga lo siguiente:

1. Compruebe que el servidor Web basado en SSL ha importado correctamente un certificado SSL.
2. Cree una copia del directorio '\$NX_ROOT/bopcfg/www/wwwroot' (incluidos los subdirectorios) y asígnele el nombre siguiente:

'\$NX_ROOT/bopcfg/www/wwwrootsec'

3. Agregue un nuevo directorio virtual para el servidor Web llamado CAisdsec. Este directorio virtual señala al directorio físico siguiente:

'\$NX_ROOT/bopcfg/www/wwwrootsec'

Verifique que los permisos del directorio virtual CAisdsec coinciden con los permisos del directorio virtual CAisd para la ejecución de scripts. Imponga SSL en el directorio virtual CAisdsec.

Nota: En este ejemplo, CAisdsec está definido por el usuario y es posible cambiar su nombre.

4. Cree un sistema sólo con un servidor primario.

Creación de sistemas sólo con servidores primarios

Puede crear un sistema que sólo utilice un servidor primario.

Nota: Para crear este sistema, debe estar instalado y configurado el servidor primario.

Para crear un sistema sólo con un servidor primario, realice lo siguiente:

1. Utilice `pdm_edit.pl` para agregar o editar las entradas de WebDirector, o las dos cosas, según lo necesite. Un solo WebDirector puede distribuir la carga entre varios motores Web. Asigne todos los motores Web y los WebDirector nuevos al host denominado principal. Este host es el servidor primario.

Nota: La función de asignación automática de la interfaz CGI de WebDirector asigna nombres desde `pdm_edit.pl`.

- Al primer WebDirector del servidor primario se le asigna de forma automática el nombre `pdmweb_d1.exe`;
- al segundo, `pdmweb_d2.exe`;
- al tercero, `'pdmweb_d3.exe'`; y así sucesivamente.

También el servidor secundario podría tener WebDirector cuyos valores de interfaz CGI fueran `pdmweb_d1.exe`, `pdmweb_d2.exe` y `pdmweb_d3.exe`. No se producen conflictos de nombres dado que los nombres de WebDirector son únicos en el equipo local donde se ejecutan.

2. Lea la información siguiente, podría aplicarse según el entorno del motor Web de su instalación CA Service Desk Manager:
 - Número de motores Web que agregar: al implementar cualquier esquema de equilibrar la carga de motor Web, el inicio de sesión SSL, o ambos, deben asignarse por lo menos dos motores Web al mismo WebDirector.
 - Entorno de inicio de sesión SSL: al definir el motor Web de inicio de sesión seguro en `pdm_edit.pl`, este motor Web debe estar sometido al control de un WebDirector. Defina el valor del parámetro correspondiente al protocolo del motor Web de inicio de sesión seguro como `https` para garantizar que WebDirector cree el valor correcto para el parámetro `RedirectingURL` del cliente Web.
3. Guarde los cambios realizados y salga de la secuencia de comandos `pdm_edit.pl`; especifique el archivo que se deba usar como plantilla `web.cfg` cuando se le solicite.

Nota: Los WebDirector no utilizan ningún archivo `'<Nombre_Host>-web[nº].cfg'`. pero los motores Web precisan un archivo `'<Nombre_Host>-web[nº].cfg'` único. Al guardar y al salir del script `pdm_edit.pl`, se generan de manera automática archivos `web.cfg` de ejemplo. Se solicita al usuario que especifique el archivo `web.cfg` que se va a usar como plantilla para la creación de los archivos de configuración Web. Es posible importar las personalizaciones del archivo `web.cfg` original a los nuevos archivos de configuración Web especificando el archivo original como archivo de plantillas deseado.

4. Copie y guarde los archivos siguientes, disponer de una copia de seguridad de estos archivos es útil por si decide restaurar el entorno original:
 - \$NX_ROOT/pdmconf/pdm_startup.tpl
 - \$NX_ROOT/pdmconf/pdm_startup
 - \$NX_ROOT/bopcfg/www/web.cfg
 - Cualquier archivo primary-web[nº].cfg existente
 - \$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml y web.xml.tpl
5. Mueva \$NX_ROOT/samples/pdmconf/pdm_startup.rmt a \$NX_ROOT/pdmconf y cambie su nombre a pdm_startup.tpl.
6. En todos los motores Web que se hayan asignado a un WebDirector, asegúrese de que se hayan definido correctamente los parámetros de WebDirector pertinentes del archivo '<Nombre_Host>-web[nº].cfg' que corresponda al motor web; para ello, examine el archivo en un editor de texto. Si es necesario, modifique los valores de los parámetros de WebDirector para que reflejen el rol del motor Web deseado. Luego cópielos en el directorio: \$NX_ROOT/bopcfg/www.
7. Mueva todos los archivos \$NX_ROOT/samples/pdmconf/primary-web[nº].cfg al directorio \$NX_ROOT/bopcfg/www.
8. Si emplea un servidor de servlet como Tomcat, la utilidad pdm_edit.pl crea archivos web.xml.tpl que sirven para sustituir el archivo web.xml.tpl en cada uno de los servidores que albergue un motor Web. Estos archivos se denominan primary-web.xml.tpl. Renombre los archivos y cópielos en el directorio:
\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF.

Si emplea un servidor HTTP como IIS o Apache, cree las copias de "pdmweb.exe" en el directorio \$NX_ROOT/bopcfg/www/wwwroot, un "pdmweb[nº].exe" para cada motor Web y un "pdmweb_d[nº].exe" para cada WebDirector definido en pdm_edit.pl. Asegúrese de que los nombres de "pdmweb[nº].exe" y "pdmweb_d[nº].exe" sigan los valores correctos de la interfaz CGI procedentes de las definiciones del script pdm_edit.pl (por ejemplo: pdmweb1.exe, pdmweb2.exe, pdmweb_d1.exe, etc.).
9. Si emplea IIS y necesita agregar extensiones de servidor para las interfaces CGI, copie el archivo primary-site.dat en el directorio \$NX_ROOT/bopcfg/www con el nombre site.dat. Cuando se vuelve a configurar el sistema, estos sitios se agregarán a IIS.
10. Vuelva a configurar el servidor principal sin reiniciar la base de datos e inicie los servicios.

11. Al finalizar la reconfiguración, compruebe si la configuración actual es válida. Inicie los demonios de CA Service Desk Manager. Compruebe que no haya ningún error en los archivos stdlog. Utilice pdm_status para consultar los demonios y su estado. Use un explorador para acceder al sistema: <http://localhost:8080/CAisd/pdmweb.exe>.
12. Para permitir que Gestión del conocimiento se integre con CA Service Desk Manager, si se ha impuesto SSL en CA Service Desk Manager, es necesario cambiar el valor del protocolo URL de CA Service Desk Manager.
 - a. En Herramientas de conocimiento, acceda a Gestor de valores, General, Integración y cambie el valor del protocolo URL de CA Service Desk Manager de "http" a "https".
 - b. Guarde los cambios y salga.
13. Abra un explorador Web por la página de inicio de sesión en CA Service Desk Manager y compruebe si pueden acceder los usuarios y si se produce el comportamiento de redirección o de inicio de sesión esperado.

Comprobación de los valores de parámetro de WebDirector

Puede verificar los valores de parámetro de WebDirector.

Para comprobar los valores de parámetro

1. En el caso de los motores Web de inicio de sesión seguro, edite el archivo `<Nombre_Host>-web[nº].cfg` del modo siguiente:
 - a. Cambie el valor de parámetro de CAisd de `/CAisd` a `/CAisdsec`.
 - b. Cambie el valor del parámetro UseDirector de Yes a AfterLogin.
 - c. Cambie el valor del parámetro Willingness de 5 a 0.
 - d. Compruebe que el valor RedirectingURL del protocolo consta como https.
 - e. Cambie el valor RedirectingURL `<directorio cgi>` de CAisd a CAisdsec.
 - f. Guarde los cambios realizados.
2. En el caso de motores no seguros que se encargan de todas las demás actividades, edite los archivos `<Nombre_Host>-web[nº].cfg` correspondientes a los motores Web no seguros que desee dedicar a las actividades no relacionadas con el inicio de sesión. Compruebe que el valor de parámetro CAisd es `/CAisd`.
 - a. Cambie el valor del parámetro UseDirector de Yes a BeforeLogin.
 - b. Mantenga el valor del parámetro Willingness en 5 o defínalo en cualquier otro valor entero del 1 al 10, según la carga en cuestión.

- c. Compruebe que el valor RedirectingURL del protocolo consta como http.
- d. Confirme que el valor RedirectingURL <directorio cgi> es CAisd.
- e. Guarde los cambios realizados.

Se comprueban los valores de parámetros de WebDirector.

Comprobación del entorno de inicio de sesión SSL

Puede comprobar el entorno del inicio de sesión de SSL para motores Web de la siguiente manera:

- Los motores Web de inicio de sesión seguro deben residir en el directorio físico asignado al directorio virtual con SSL impuesto (CAisdsec en este ejemplo).

En el caso de los motores Web de inicio de sesión seguro, cree instancias de pdmweb.exe en el directorio \$NX_ROOT/bopcfg/www/wwwrootsec con el nombre pdmweb[nº].exe. El nombre del ejecutable debe coincidir con el valor de la interfaz CGI que corresponda a cada uno de los motores Web de inicio de sesión seguro definidos en pdm_edit.pl.

Por ejemplo: si se ha asignado a pdm_edit.pl el valor de la interfaz CGI del motor Web de inicio de sesión seguro a pdmweb2, cree una copia física de pdmweb.exe y cámbiele el nombre a pdmweb2.exe.

- Los WebDirector y motores Web no seguros deben residir en el directorio físico asignado al directorio virtual no SSL CAisd.

En el caso de los WebDirector y motores Web no seguros cree nuevas instancias de pdmweb.exe en el directorio \$NX_ROOT/bopcfg/www/wwwroot. Es necesario que exista una copia de pdmweb.exe por cada WebDirector y motor Web no seguro que se haya definido en pdm_edit.pl. Cambie el nombre de las copias para que los nombres nuevos de los archivos ejecutables coincidan con los valores de la interfaz CGI definidos para los motores Web y los WebDirector en pdm_edit.pl.

Por ejemplo: si se ha asignado a pdm_edit.pl el valor de la interfaz CGI de pdmweb3 al motor Web no seguro y el valor pdmweb_d1 a WebDirector, cree dos copias de pdmweb.exe. Cambie el nombre de la primera copia a pdmweb3.exe y luego cambie el nombre de la segunda copia a pdmweb_d1.exe.

Capacidades Web y servidores secundarios

Todos los sistemas tienen un servidor primario. Dicho servidor alberga los servicios del sistema principal, como el concentrador de comunicaciones y la base de datos. Muchos usuarios de la empresa extienden el sistema a otros servidores, denominados servidores secundarios. En este tipo de configuración, es posible agregar capacidades Web a los servidores secundarios.

Cómo preparar capacidades Web

Las tareas requeridas previamente para agregar capacidades a servidores secundarios (y si va a implementar un entorno de inicio de sesión SSL) son las siguientes:

1. Compruebe que estén instalados y configurados los servidores primarios y secundarios.
2. Verifique que el servidor Web basado en SSL que vaya a albergar el motor Web de inicio de sesión seguro haya importado un certificado SSL.
3. En el servidor Web que alberga el motor Web de inicio de sesión seguro, cree una copia física del directorio `$NX_ROOT/bopcfg/www/wwwroot` (incluidos los subdirectorios) y llámelo `$NX_ROOT/bopcfg/www/wwwrootsec`.
4. Defina un nuevo directorio virtual para el servidor Web llamado CAisdsec.
5. Haga que el directorio virtual apunte al directorio físico `$NX_ROOT/bopcfg/www/wwwrootsec`.
6. Verifique que los permisos del directorio virtual CAisdsec coinciden con los permisos del directorio virtual CAisd para la ejecución de scripts.
7. Imponga SSL en el directorio virtual CAisdsec.

Nota: El nombre CAisdsec es definido por el usuario y se puede cambiar.

Creación de sistemas con servidores secundarios

Para crear un sistema con servidores secundarios, realice lo siguiente:

1. Utilice `pdm_edit.pl` para agregar o editar las entradas de WebDirector. Un solo WebDirector puede distribuir la carga entre varios motores Web. Agregue motores Web y WebDirectors a otros servidores. Al especificar servidores secundarios, debe emplear el mismo nombre con el que se configuraron. Este nombre es el valor `NX_LOCAL_HOST` del archivo `NX.env` ubicado del servidor secundario en cuestión.

Nota: La asignación automática de la interfaz CGI de WebDirector asigna los nombres desde `pdm_edit.pl`: al primer WebDirector del servidor primario se le asigna automáticamente el nombre `pdmweb_d1.exe`; al segundo, `pdmweb_d2.exe`; al tercero, `pdmweb_d3.exe`; y así sucesivamente. También el servidor secundario podría tener WebDirector cuyos valores de interfaz CGI fueran `pdmweb_d1.exe`, `pdmweb_d2.exe` y `pdmweb_d3.exe`. No se producen conflictos de nombres dado que los nombres de WebDirector son únicos en el equipo local donde se ejecutan.

2. Cada uno de los motores Web debe hacer referencia a un gestor de objetos. Siempre hay un gestor de objetos denominado `domsrvr`. Se pueden agregar más gestores de objetos en los servidores secundarios y luego asignarles motores Web de la siguiente manera:
 - Número de motores Web que agregar: al implementar cualquier esquema de equilibrar la carga de motor Web, el inicio de sesión SSL, o ambos, asigne por lo menos dos motores Web al mismo WebDirector.
 - Entorno de inicio de sesión SSL: al definir el motor Web de inicio de sesión seguro en `pdm_edit.pl`, este motor Web debe estar sometido al control de un WebDirector. Defina el valor del parámetro correspondiente al protocolo del motor Web de inicio de sesión seguro como `https`. Esta configuración hace que WebDirector cree el valor `RedirectingURL` correcto para el cliente Web.
3. Guarde los cambios realizados, salga del script `pdm_edit.pl` y especifique el archivo que se deba usar como plantilla `web.cfg` cuando se le solicite.

Nota: Los WebDirector no utilizan ningún archivo `<Nombre_Host>-web[nº].cfg`. No obstante, los motores Web requieren un archivo `<Nombre_Host>-web[nº].cfg` único. Al guardar y al salir del script `pdm_edit.pl`, se generan de manera automática archivos `web.cfg` de ejemplo. Se solicita al usuario que especifique el archivo `web.cfg` que se va a usar como plantilla para la creación de los archivos de configuración Web. Puede importar las personalizaciones del archivo `web.cfg` original a los archivos de configuración web nuevos especificando el archivo `web.cfg` original como archivo de plantillas que desea utilizar.

4. En el servidor primario, guarde las copias de seguridad siguientes. Resultan útiles si se desea restaurar el entorno original:
\$NX_ROOT/pdmconf/pdm_startup.tpl
\$NX_ROOT/pdmconf/pdm_startup
\$NX_ROOT/bopcfg/www/*web*.cfg
\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*
5. En los servidores secundarios, guarde copias de seguridad de los archivos \$NX_ROOT/bopcfg/www/web.cfg o <nombre_secundario>-web[nº].cfg existentes.
\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*
6. En los servidores primarios, mueva \$NX_ROOT/samples/pdmconf/pdm_startup.rmt a \$NX_ROOT/pdmconf y cambie su nombre a pdm_startup.tpl.
7. Para cada motor Web que se asigna a un WebDirector, compruebe si se han definido correctamente los parámetros de WebDirector pertinentes del archivo <Nombre_Host>-web[nº].cfg que corresponda al motor Web; para ello, examine el archivo en un editor de texto. Si es necesario, modifique los valores de los parámetros de WebDirector para especificar el rol del motor Web deseado.
8. En el servidor principal, mueva todos los archivos \$NX_ROOT/samples/pdmconf/primary-web[nº].cfg al directorio \$NX_ROOT/bopcfg/www.
9. Mueva todos los archivos \$NX_ROOT/samples/pdmconf/'secondary_server_name-web[nº].cfg del servidor primario al directorio \$NX_ROOT/bopcfg/www de los servidores secundarios.
10. (Servidores de servlet como Tomcat) Especifique un web.xml.tpl en cada directorio de \$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF. Cuando se configura el servidor, el propio proceso de configuración crea un archivo web.xml. La utilidad pdm_edit.pl crea archivos web.xml.tpl de ejemplo, cuyo nombre sigue la estructura <nombredehost>-web.xml.tpl. Estos archivos se pueden utilizar como ejemplo: copie y cambie su nombre a web.xml.tpl en todos los servidores.
11. (Servidores HTTP como IIS o Apache) En cada servidor de CA Service Desk Manager (primario, secundario, o ambos) que aloje un motor Web o WebDirector, cree copias de pdmweb.exe en el directorio \$NX_ROOT/bopcfg/www/wwwroot. En pdm_edit.pl se define un pdmweb[nº].exe para cada motor Web y un pdmweb_d[nº].exe para cada WebDirector que se ejecuta en ese servidor. Compruebe que pdmweb[nº].exe y pdmweb_d[nº].exe están denominados con los valores de la interfaz CGI desde las definiciones del script de pdm_edit.pl (por ejemplo, pdmweb1.exe, pdmweb2.exe, pdmweb_d1.exe, etc.).

12. Si emplea IIS y necesita agregar extensiones de servidor para cada interfaz CGI, copie el archivo `primary-site.dat` en el directorio `$NX_ROOT/bopcfg/www` con el nombre `site.dat`. Cuando se vuelve a configurar el sistema, estos sitios se agregarán a IIS.
13. Vuelva a configurar el servidor primario sin reiniciar la base de datos e inicie los servicios.
14. Vuelva a configurar cada uno de los servidores secundarios.
15. Para permitir que Gestión del conocimiento se integre con CA Service Desk Manager, si se ha impuesto SSL en CA Service Desk Manager, es necesario cambiar el valor del protocolo URL de CA Service Desk Manager.
 - a. En Gestión del conocimiento, Gestor de valores, General, cambie el valor del protocolo URL de CA Service Desk Manager de "http" a "https".
 - b. Guarde los cambios y salga.
16. Abra un explorador Web por la página de inicio de sesión en CA Service Desk Manager y compruebe si pueden acceder los usuarios y si se produce el comportamiento de redirección o de inicio de sesión esperado.

Configuración del servidor

`pdm_edit.pl` permite agregar funciones y aumentar el rendimiento del sistema de la empresa. Puede configurar los servicios de CA Service Desk Manager. CA Service Desk Manager tiene distintos daemon básicos en el servidor primario. Puede agregar más daemon en el servidor primario y, a continuación, el sistema se puede extender a varios servidores agregando servidores secundarios, que aumentan el volumen y el rendimiento, y mejoran la seguridad.

Si utiliza `pdm_edit.pl` para modificar la configuración de daemon, las personalizaciones disponibles con `pdm_configure` estarán deshabilitadas. Por ejemplo, tras modificar el archivo `pdm_startup.tpl` con la utilidad `pdm_edit.pl`, no se puede activar ningún WebDirector ni ningún conversor de eventos en la interfaz gráfica de usuario de `pdm_configure`. Puede personalizar dichas funciones con la utilidad `pdm_edit.pl`.

El menú superior de `pdm_edit.pl` aparece después de haber ejecutado `pdm_edit.pl` y haber introducido un par de preguntas específicas del sistema operativo. En este menú figuran las capacidades de esta utilidad. Al introducir un número desde este menú se accede a submenús propios de la función seleccionada. Desde estos submenús, se puede regresar al menú superior. Al final de la sesión, debe seleccionar entre "Quit NO SAVE" o "Save and quitW". Esta acción creará un archivo `pdm_startup.dat` que es un resumen de todas las selecciones realizadas. Guarde este archivo; se puede reanudar más adelante. La utilidad crea un archivo `pdm_startup.rmt` y sirve como sustituto del archivo `$NX_ROOT/pdmconf/pdm_startup.tpl` del servidor primario. Una vez instalado el archivo `pdm_startup.rmt` como `pdm_startup.tpl` en el servidor primario, vuelva a configurar la base de datos, pero sin reinicializarla, para activar los cambios.

Nota: En el nombre de host de todos los servidores secundarios se distingue entre mayúsculas y minúsculas, y representa el valor de `NX_LOCAL_HOST` en el archivo `NX.env` del servidor secundario.

Ejecución de `pdm_edit.pl` en servidores de UNIX

Puede ejecutar `pdm_edit.pl` en servidores de UNIX. Debe disponer de una instalación de servidor primario y, opcionalmente, un servidor secundario instalado y configurado para todos los documentos pertinentes de CA Service Desk Manager.

Nota: Ejecute `pdm_edit.pl` únicamente en el servidor primario. Para obtener más información acerca de servidores secundarios que ejecutan la interfaz Web, consulte la *Guía de implementación*.

Para ejecutar `pdm_edit.pl` en un servidor de UNIX

1. En la línea de comandos del servidor primario, cambie a la ubicación siguiente:

```
$NX_ROOT/samples/pdmconf
```

2. Emita el siguiente comando:

```
'$NX_ROOT/bin/pdm_perl pdm_edit.pl'
```

El archivo ejecutable `pdm_perl` de CA Service Desk Manager ejecuta el script `pdm_edit.pl`. Una serie de preguntas y selecciones de menú en texto le permite agregar, modificar o suprimir gestores de objetos, WebDirector y motores Web, así como guardar los cambios o las adiciones en archivos `pdm_startup.dat` y `pdm_startup.rmt` del servidor primario.

Ejecución de pdm_edit.pl en servidores de Windows

Puede ejecutar pdm_edit.pl en servidores de UNIX. Debe disponer de una instalación de servidor primario y, opcionalmente, un servidor secundario instalado y configurado para todos los documentos pertinentes de CA Service Desk Manager.

Nota: Ejecute pdm_edit.pl únicamente en el servidor primario. Para obtener más información acerca de servidores secundarios que ejecutan la interfaz Web, consulte la *Guía de implementación*.

Para ejecutar pdm_edit.pl en un servidor de Windows

1. Abra una ventana del símbolo del sistema y acceda al directorio siguiente:

```
%directorio-instalación\samples\pdmconf.
```

2. Emita el siguiente comando:

```
%directorio-instalación\bin\pdm_perl pdm_edit.pl
```

El archivo ejecutable pdm_perl de CA Service Desk Manager ejecuta el script pdm_edit.pl. Una serie de preguntas y selecciones de menú en texto le permite agregar, modificar o suprimir gestores de objetos, WebDirector y motores Web, así como guardar los cambios o las adiciones en archivos pdm_startup.dat y pdm_startup.rmt del servidor primario.

Gestores de objetos

Como su propio nombre indica, los gestores de objetos se ocupan de gestionar todos los objetos de CA Service Desk Manager. Siempre hay un gestor de objetos en el servidor primario. Todos los gestores de objetos poseen un nombre, que es el que usan para comunicarse con los demás objetos. El gestor de objetos predeterminado del servidor primario se llama siempre domsrvr. En los sistemas empresariales que dispongan de servidores de procesamiento múltiple o servidores secundarios, es posible agregar más gestores de objetos tanto al servidor primario como a los servidores secundarios. Puede desplazarse, agregar, editar y suprimir gestores de objetos.

A todos los gestores de objetos se les asigna un host. Los gestores de objetos asignados al servidor primario siempre indican primary como nombre del host.

Puede agrupar los gestores de objeto para que los grupos puedan ser asignados y ofrecer el servicio a grupos específicos de motores Web y clientes Java. Normalmente, puede no especificarse ningún *grupo* y dejar que la función para equilibrar la carga del sistema sea la que reparta la carga entre todos los gestores de objetos. Los usuarios que se valen de esta función suelen emplear motores Web distantes geográficamente del servidor primario, por lo que es conveniente ubicar algún gestor de objetos cerca del motor adecuado. Los usuarios agrupan los gestores de objetos que están asignados a los motores Web locales y, a continuación, asignan estos últimos al grupo de gestores de objetos.

La máscara de aceptación es una función avanzada que indica al gestor de objetos de qué clientes debe aceptar conexiones. Por lo general, los motores Web intentan conectarse a los gestores de objetos con nombres como `web:seattle:1`, `web:seattle:2` o `web:texas:1`. El administrador puede especificar una máscara de aceptación como `web:seattle.*` para aceptar todas las conexiones de seattle y rechazar otras. El administrador también puede especificar la máscara `web:.*`, por ejemplo, para que se acepten las conexiones de los motores Web y se rechacen las de los clientes.

El valor de visualización resulta de gran utilidad en algunas ocasiones. Los usuarios, en su gran mayoría, permiten que el sistema adopte este valor predeterminado, que coincide con el nombre del host. Dicho valor aparece en los clientes para indicar el gestor de objetos al que se ha conectado.

Acceso y salida del gestor de objetos

La instalación de CA Service Desk Manager proporciona, de forma predeterminada, un gestor de objetos al servidor primario. El gestor de objetos predeterminado (`comm`). En la lista del gestor de objetos, no figura `name = 'domsrvr'`, pero hay que tener en cuenta que está presente y que se inicia al iniciar el gestor de daemon de CA Service Desk Manager.

Procedimiento para entrar y salir del gestor de objetos

1. En el menú superior de `pdm_edit.pl`, seleccione 1 y pulse Intro.

Aparecerá el submenú Gestor de objetos.

2. Pulse la tecla Intro.

Al salir del submenú Gestor de objetos, vuelve a aparecer el menú de nivel superior `pdm_edit.pl`.

Adición de gestores de objetos

Puede agregar gestores de objetos al submenú Gestor de objetos.

Procedimiento para agregar gestores de objetos

1. En el submenú Gestor de objetos, seleccione a y pulse la tecla Intro.

El sistema solicita el nombre de host.

2. Pulse la tecla Intro para seleccionar el valor predeterminado del servidor primario o escriba el valor correspondiente al nombre del host del servidor secundario oportuno.

Nota: El nombre de host de todos los servidores secundarios distingue entre mayúsculas y minúsculas y es el valor de NX_LOCAL_HOST en el archivo NX.env del servidor secundario.

3. Pulse la tecla Intro.

El sistema solicita el grupo.

4. Pulse la tecla Intro si desea aceptar el valor predeterminado (ninguno) o escriba el nombre del grupo que le interese y, a continuación, pulse la tecla Intro.

El sistema solicita la máscara de aceptación.

Nota: Las máscaras de aceptación son filtros que restringen la comunicación de los gestores de objetos a los procesos cuyo nombre coincida con la máscara.

5. Pulse la tecla Intro si desea aceptar el valor predeterminado (no aceptar) o escriba la cadena de la máscara de aceptación que desee utilizar.

El sistema solicita el valor de Nombre de visualización del panel de resultados.

6. Pulse la tecla Intro si desea aceptar el valor predeterminado o escriba el nombre de visualización que le interese y, a continuación, pulse la tecla Intro.

Aparecerá el submenú Gestor de objetos con el gestor de objetos recientemente agregado ya incluido.

Edición de gestores de objetos

Puede editar los gestores de objetos.

Procedimiento para editar gestores de objetos

1. En el submenú Gestor de objetos, seleccione e y pulse la tecla Intro.

El sistema solicita que introduzca la clave.

Nota: Este valor de clave se muestra en la lista de gestores de objetos y se crea de forma automática cada vez que se agrega algún gestor de objetos. La clave adopta el formato "nombredehost: nº". nº es un entero en orden secuencial; el número más alto de la secuencia coincide con el número total de gestores de objetos presentes en el host especificado. Por ejemplo, si existen dos gestores de objetos en el servidor primario y otros dos gestores en un servidor secundario (cuyo nombre de host es "godzilla"), las claves correspondientes serían: "primary:1", "primary:2", "godzilla:1" y "godzilla:2".

2. Introduzca la clave (godzilla:1) deseada y pulse la tecla Intro.

El sistema solicita el Grupo.

3. Pulse la tecla Intro si desea aceptar el valor mostrado "tal cual" o modifíquelo indicando otro valor para el grupo y pulsando la tecla Intro.

El sistema solicita la máscara de aceptación.

4. Pulse la tecla Intro si desea aceptar el valor mostrado "tal cual" o modifíquelo indicando otro valor para la máscara de aceptación y pulsando la tecla Intro.

El sistema solicita Visualización.

5. Pulse la tecla Intro si desea aceptar el valor mostrado "tal cual" o modifíquelo indicando otro valor para la visualización y pulsando la tecla Intro.

El submenú Gestor de objetos aparece y el gestor de objetos es editado.

Eliminación de gestores de objetos

Los gestores de objetos se pueden suprimir.

Procedimiento para suprimir gestores de objetos

1. En el submenú Gestor de objetos, seleccione d y pulse la tecla Intro.
El sistema solicita que introduzca la clave.
2. Introduzca la clave deseada y pulse la tecla Intro.

Nota: Si ha introducido una clave incorrecta (que podría suprimir la entrada de domsrvr equivocada), salga de la secuencia de comandos pdm_edit.pl *sin* guardar los cambios realizados.

El gestor de objetos queda suprimido y vuelve a aparecer el submenú Gestor de objetos.

Especificación de WebDirector

Los WebDirector son opcionales y se utilizan cuando los sistemas requieren dos o más motores Web. Los WebDirector se ocupan de equilibrar la carga entre los motores Web. Puede no haber ninguno o haber varios WebDirectors. Si los hay, cada uno de ellos equilibra la carga entre dos o más motores Web.

Para especificar un WebDirector, realice los pasos siguientes:

1. Indique el nombre de host.
Si se encuentra en el servidor primario, escriba "primary"; de lo contrario, escriba el nombre del servidor secundario oportuno. El nombre del servidor secundario es la entrada NX_LOCAL_HOST del archivo NX.env en el servidor secundario.
Nota: Tenga en cuenta la distinción entre mayúsculas y minúsculas.
2. (Opcional) Especifique la interfaz CGI.
En la mayoría de los casos, el valor predeterminado es adecuado. Si emplea un servidor HTTP como IIS o Apache, este valor es el ejecutable de CGI que se ejecuta en respuesta a las solicitudes de CGI (el nombre del archivo ejecutable de CGI). Cree copias del archivo pdmweb.exe en el directorio \$NX_ROOT/bopcfg/www/wwwroot con dicho nombre. Si emplea un servidor servlet como Tomcat, se crea un archivo web.xml.tpl de ejemplo, que sirve para sustituir el archivo web.xml.tpl del directorio \$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF que corresponda al servidor concreto. Todos los archivos web.xml.tpl de ejemplo se crean en el directorio actual y se nominan según la estructura <nombredehost>-web.xml.tpl.

Acceso y salida de WebDirector

Al definir un WebDirector, tan sólo se agrega su información. CA Service Desk Manager sólo lo utiliza si se le asigna al menos un motor Web. Puede acceder y salir de WebDirector.

Procedimiento para acceder y salir de WebDirector

1. En el menú superior de pdm_edit.pl, seleccione d y pulse Intro.
Aparecerá el submenú WebDirector.
2. Pulse la tecla Intro.
Al salir del submenú WebDirector, vuelve a aparecer el menú de nivel superior pdm_edit.pl.

Cómo agregar WebDirector

Puede agregar otros WebDirector. Cada uno de los WebDirector definidos en pdm_edit.pl debe disponer de un valor único de interfaz CGI. El nombre de la interfaz CGI se genera de manera automática, pero el nombre sugerido para la misma se puede sustituir manualmente a fin de que se ajuste a los esquemas de nomenclatura de CGI que desee.

Considere lo siguiente antes de agregar cualquier WebDirector:

- Si emplea un servidor HTTP como IIS o Apache, debe haber un ejecutable pdmweb_d[nº].exe con el nombre correcto en el directorio \$NX_ROOT/bopcfg/www/wwroot.
- Si emplea un servidor de servlet como Tomcat, se obtiene un archivo web.xml.tpl de ejemplo, cuyo nombre sigue la estructura *<nombredehost>-web.xml.tpl* y se ubica en el directorio de trabajo. Este archivo sirve para sustituir el archivo \$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml.tpl que corresponda al servidor concreto.

Procedimiento para agregar WebDirector

1. En el submenú WebDirector, seleccione a y pulse la tecla Intro.
El sistema solicita el nombre de host.
2. Pulse la tecla Intro para seleccionar el valor predeterminado del servidor principal o escriba el valor correspondiente al nombre del host del servidor secundario oportuno.
3. Pulse la tecla Intro.
El sistema solicita un nombre para la interfaz CGI.

4. Pulse la tecla Intro si desea aceptar el valor mostrado o escriba el valor que le interese y, a continuación, pulse la tecla Intro.

Aparecerá el submenú WebDirector con el WebDirector que se ha agregado recientemente incluido.

Edición de WebDirector

Los WebDirector se pueden editar.

Procedimiento para editar un Web Director

1. En el submenú WebDirector, seleccione e y pulse la tecla Intro.
El sistema solicita que introduzca la clave.
2. Introduzca la clave deseada y pulse la tecla Intro.
El sistema solicita un valor de interfaz CGI.
3. Pulse Intro para aceptar el valor mostrado o modifique el valor introduciendo el valor de interfaz CGI deseado y pulse la tecla Intro.
Aparecerá el submenú WebDirector y WebDirector queda cambiado.

Eliminación de un WebDirector

Es posible suprimir una entrada de WebDirector.

Procedimiento para suprimir entradas de WebDirector

1. En el submenú WebDirector, seleccione d y pulse la tecla Intro.
El sistema solicita que introduzca la clave.
2. Introduzca la clave deseada y pulse la tecla Intro.
Nota: Si ha introducido una clave incorrecta (que podría suprimir la entrada equivocada WebDirector), salga de la secuencia de comandos `pdm_edit.pl` sin guardar los cambios realizados.
Aparecerá el submenú WebDirector y WebDirector queda suprimido.

Cambio del valor de la interfaz CGI de WebDirector

Es posible cambiar el valor de la interfaz CGI en los WebDirector.

Procedimiento para cambiar el valor de CGI/IF

1. En el submenú WebDirector, seleccione c y pulse la tecla Intro.
El sistema solicita que introduzca la clave.
2. Introduzca la clave deseada y pulse la tecla Intro.
El sistema solicita un valor de interfaz CGI.

3. Pulse la tecla Intro si desea aceptar el valor mostrado tal como está o modifíquelo indicando otro valor para la interfaz CGI y, a continuación, pulse la tecla Intro.

Aparecerá el submenú WebDirector y el valor de interfaz CGI para WebDirector queda cambiado.

Motores Web

Los motores Web ayudan a preparar las páginas Web para el cliente Web. Todos los sistemas tienen, como mínimo, un motor Web. En cada servidor puede haber cero o más motores Web. Puede desplazarse, agregar, editar y suprimir motores Web. Cada uno de los motores Web se conecta a un gestor de objetos para iniciar el procesamiento de todas las solicitudes de objetos de CA Service Desk Manager. El comportamiento por defecto consiste en conectarse al gestor de objetos predeterminado pero, si existe más de un gestor, se puede definir este valor como ANY.

Al definir un motor Web, es necesario especificar el nombre del host correspondiente. Introduzca **primary** para todos los motores Web que se inician en el servidor primario; de otro modo, especifique el nombre de host del servidor secundario. Este nombre, que distingue entre mayúsculas y minúsculas, debe coincidir con el valor de la entrada NX_LOCAL_HOST del archivo NX.env ubicado en el servidor secundario pertinente.

Es posible ejecutar los motores Web y acceder a ellos directamente. En el acceso directo, cada explorador Web introduce la interfaz CGI específica para ese motor Web y los usuarios determinan la carga del sistema (la función de equilibrar la carga no está automatizada). Todos los clientes se pueden conectar a un solo motor Web y saturarlo, mientras que otros motores no están en uso. Un mejor enfoque es asignar dos o más motores Web a un solo WebDirector. Así, todas las solicitudes que, en principio, se dirigen a uno de estos motores Web son redirigidas al WebDirector para que equilibre la carga y las redirija al motor Web con mayor disposición del grupo.

Otras configuraciones pueden incluir WebDirector. En una de ellas, todos los inicios de sesión se dirigen a un solo motor Web SSL seguro que se ocupa de gestionar esta actividad. Tras el inicio de la sesión, los clientes se dirigen a otros motores Web disponibles para el resto del procesamiento.

Interfaz CGI

Todos los motores Web disponen y utilizan una interfaz CGI como sigue:

- Si emplea un servidor HTTP como IIS o Apache, la interfaz es el ejecutable que se encuentra almacenado en el directorio \$NX_ROOT/bopcfg/www/wwwroot. El nombre de la interfaz CGI es el nombre del ejecutable. Los exploradores indican la interfaz CGI en la línea de dirección y la petición se dirige al motor Web apropiado.

- Si emplea un servidor servlet como Tomcat, la interfaz CGI se simula por medio de un servlet. Cada servidor servlet cuenta con un archivo web.xml.tpl que describe todas las interfaces CGI. La utilidad pdm_edit.pl crea archivos web.xml.tpl de ejemplo, cuyo nombre sigue la estructura <nombredehost>-web.xml.tpl. Estos archivos sirven para sustituir el archivo web.xml.tpl del servidor pertinente y volver a configurar el servidor.
- Cuando se utiliza WebDirector, a menudo resulta útil definir la interfaz GI de los motores Web con un nombre GI conocido. Así, todas las solicitudes van a dicho motor y se redirigen a otro motor Web con mayor disponibilidad. Esta configuración permite que los usuarios sólo hayan de recordar un único nombre de interfaz CGI y que todas las solicitudes se repartan entre todos los motores Web disponibles.

Entrada y salida de motores Web

La instalación de CA Service Desk Manager instala y configura de forma predeterminada un motor Web en el servidor primario (clave = primary:1; gestor de objetos = domsrvr; interfaz CGI = "pdmcgi"; protocolo = sin especificar).

Procedimiento para entrar y salir de motores Web

1. En el menú superior de pdm_edit.pl, seleccione w y pulse Intro.

Aparecerá el submenú Motor Web.

2. Pulse la tecla Intro.

Al salir del submenú Motor Web, vuelve a aparecer el menú de nivel superior pdm_edit.pl.

Consideraciones para agregar motores Web

Considere la información siguiente cuando agregue motores Web:

- **Dirigir los clientes a motores Web:** puede especificar cómo se dirigen los clientes Web a motores Web. Por ejemplo, suponga que se están usando dos WebDirector: miko:1 y godzilla:1. miko:1 tiene cuatro motores Web asignados: godzilla:1, godzilla:2, godzilla:3 y primary:3. Cualquier cliente Web puede solicitar `https:godzilla:8080/Caisd/ComputerAssociates.exe` y ser redireccionado a cualquiera de los cuatro motores Web de ese grupo. Si el cliente Web especifica `http://hostlocal:8080/Caisd/pdmweb6.exe`, siempre se dirigirá a este motor Web. Fíjese, asimismo, en que algunos de los motores Web están asignados al gestor de objetos llamado domsrvr y otros están configurados para conectarse a cualquier gestor de objetos.
- **Uso de valores de la interfaz CGI:** cada uno de los motores Web definido en `pdm_edit.pl` debe tener un valor de interfaz CGI único:
 - Si emplea un servidor HTTP como IIS o Apache, debe tener un ejecutable `pdmweb[nº].exe` con el nombre correcto en el directorio `$NX_ROOT/bopcfg/www/wwwroot`.
 - Si emplea un servidor de servlet como Tomcat, la interfaz CGI se reemplaza por un servlet. Estos servidores deben contar con un archivo `web.xml.tpl` en el directorio `$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/Caisd/WEB-INF` que describa las interfaces CGI. La utilidad `pdm_edit.pl` crea archivos `web.xml.tpl` de ejemplo, cuyo nombre sigue la estructura `<nombredehost>-web.xml.tpl`. Éstos sirven para reemplazar el archivo `web.xml.tpl` y volver a configurar el servidor.

Adición de motores Web

Puede agregar otros motores Web.

Procedimiento para agregar motores Web

1. En el submenú Motor Web, seleccione a y pulse la tecla Intro.
El sistema solicita el nombre de host.
2. Pulse la tecla Intro para seleccionar el valor predeterminado del servidor principal o escriba el valor correspondiente al nombre del host del servidor secundario oportuno.
3. Pulse la tecla Intro.
El sistema solicita el nombre del gestor de objetos.
4. Pulse la tecla Intro si desea aceptar el valor predeterminado (`<primary domsrvr>`) o escriba la combinación adecuada de alias y nombres de comunicación de domsrvr y, a continuación, pulse la tecla Intro.
El sistema solicita la clave del directorio Web.

5. Pulse la tecla Intro para seleccionar el valor predeterminado Null (ningún WebDirector) o indique uno de los que se muestran como valor de la clave y, a continuación, pulse la tecla Intro.

El sistema solicita el nombre para la interfaz CGI.

6. Pulse la tecla Intro si desea aceptar el valor mostrado o escriba el valor manualmente y, a continuación, pulse la tecla Intro.

Si no se ha especificado ningún WebDirector para este motor Web, aparecerá el submenú Motor Web. Si se ha especificado algún valor de WebDirector o ya existía uno en la definición del motor, aparece un mensaje donde se le pide que especifique el protocolo que se debe usar delante de la dirección URL de redirección del motor Web.

7. Pulse la tecla Intro si no desea colocar ningún prefijo de protocolo delante del valor de la dirección URL de redirección.
8. Introduzca **http** para anteponer el prefijo de protocolo http al valor de redirección a menos que se imponga SSL en el motor Web. Por ejemplo, introduzca **https** para anteponer el prefijo de protocolo https al valor de redirección.

Nota: Si se ha definido algún WebDirector para el motor Web, WebDirector controla la redirección al motor Web mediante el valor del parámetro RedirectingURL. Si no se va a usar el protocolo SSL en el motor Web, especifique "**http**" o no especifique ninguno. Si el protocolo SSL se va a imponer para este motor Web, especifique "**https**". Si no se hace, podría fallar el intento de redirección de WebDirector.

9. Pulse la tecla Intro.

Aparecerá el submenú Motor Web con el motor Web que se ha agregado recientemente incluido.

Edición de motores Web

Los motores Web se pueden editar.

Procedimiento para editar un motor Web

1. En el submenú Motor Web, seleccione e y pulse la tecla Intro.

El sistema solicita que introduzca la clave.

2. Introduzca la clave deseada y pulse la tecla Intro.

El sistema solicita que se introduzca el gestor de objetos.

3. Pulse la tecla Intro si desea aceptar el valor mostrado tal como está o modifíquelo indicando otro valor de gestor de objetos y, a continuación, pulse la tecla Intro.

El sistema solicita un WebDirector.

4. Pulse la tecla Intro si desea aceptar el valor mostrado tal como está o modifíquelo indicando otro valor de WebDirector y, a continuación, pulse la tecla Intro.

El sistema solicita un valor de interfaz CGI.

5. Pulse la tecla Intro si desea aceptar el valor mostrado tal como está o modifíquelo indicando otro valor para la interfaz CGI y, a continuación, pulse la tecla Intro.

El sistema solicita el protocolo HTTP.

6. Pulse la tecla Intro si desea aceptar el valor mostrado tal como está o modifíquelo indicando el valor de protocolo HTTP deseado y, a continuación, pulse la tecla Intro.

Aparecerá el submenú Motor Web.

Eliminación de motores Web

Puede suprimir un motor Web.

Procedimiento para eliminar un motor Web

1. En el submenú Motor Web, seleccione d y pulse la tecla Intro.

El sistema solicita que introduzca la clave.

2. Introduzca la clave deseada y pulse la tecla Intro.

Nota: Si ha introducido una clave incorrecta (que podría suprimir la entrada equivocada del motor Web), salga de la secuencia de comandos `pdm_edit.pl` sin guardar los cambios realizados.

El motor Web queda suprimido y aparece el submenú Motor Web.

Introducción de cambios mediante `pdm_edit.pl`

Puede hacer uso de la utilidad `pdm_edit.pl` para agregar y mover conversores, servidores, daemons y alias en el sistema CA Service Desk Manager.

Adición de conversores de TNG

La utilidad `pdm_edit.pl` permite agregar un solo conversor de TNG a cualquier servidor del sistema.

Nota: Si el gestor de daemon gestiona el conversor de TNG; este daemon se inicia y se detiene con los otros daemon. Si se requiere que el conversor de TNG capte eventos después de que los daemon de CA Service Desk Manager se hayan apagado, el conversor de TNG no puede satisfacer este requisito, por tanto, debe iniciar y detener el conversor de TNG como servicio.

Procedimiento para agregar conversores de TNG

1. En el menú superior de `pdm_edit.pl`, seleccione T y pulse la tecla Intro.
Aparecerá el submenú Conversor de TNG.
2. En el submenú Conversor de TNG, seleccione A y pulse la tecla Intro.
El sistema solicita un nombre de host.
3. Especifique **primary** para el servidor primario o el nombre del host adecuado si se trata de un servidor secundario, y luego pulse la tecla Intro.
El sistema solicita una dirección IP.
4. Introduzca **HOST_IP_REPLACE** si el conversor de TNG está en el servidor primario; de otro modo, introduzca la dirección IP del servidor secundario.
El conversor de TNG queda agregado al servidor.

Adición de conversores de UNIX

La utilidad `pdm_edit.pl` permite agregar un solo conversor de UNIX a cualquier servidor del sistema.

Procedimiento para agregar conversores de UNIX

1. En el menú superior de `pdm_edit.pl`, seleccione N y pulse la tecla Intro.
Aparecerá el submenú Conversor de UNIX.
2. Seleccione A y pulse la tecla Intro.
El sistema solicita un nombre de host.
3. Especifique **primary** para el servidor primario o el nombre del host adecuado si se trata de un servidor secundario, y luego pulse la tecla Intro.
El sistema solicita una dirección IP.
4. Introduzca **HOST_IP_REPLACE** si el conversor de UNIX está en el servidor primario; de otro modo, introduzca la dirección IP del servidor secundario.
El conversor de UNIX queda agregado al sistema.

Movimiento de validación de inicios de sesión

El servidor de validación de inicios de sesión utiliza el sistema operativo local para validar las solicitudes de los usuarios. El daemon de validación se inicia en el servidor primario de forma predeterminada, pero puede trasladarse a un servidor secundario en el que todos los usuarios tienen cuentas de sistema operativo, o a un servidor que tenga un tipo de sistema operativo diferente.

Procedimiento para mover la validación de inicios de sesión

1. En el menú superior de pdm_edit.pl, seleccione U y pulse la tecla Intro.
Aparecerá el submenú del servidor Validación de usuarios.
2. Introduzca **E** para especificar el nombre de host del servidor y pulse la tecla Intro.
3. Escriba **primary** para el servidor primario o el nombre del host adecuado si se trata de un servidor secundario, y luego pulse la tecla Intro.
La validación de inicios de sesión queda trasladada.

Traslado del servidor LDAP

El Protocolo LDAP (Lightweight Directory Access) se instala en el servidor primario de forma predeterminada, pero puede moverse a cualquier servidor secundario.

Procedimiento para mover el servidor LDAP

1. En el menú superior de pdm_edit.pl, seleccione L y pulse la tecla Intro.
Aparecerá el submenú Servidor LDAP.
2. Introduzca **E** para especificar el nombre de host del servidor o introduzca **primary** para el servidor primario o el nombre de host del servidor secundario.
El servidor LDAP queda trasladado.

Adición de demonios de repositorio

De forma predeterminada, existe un daemon de repositorio en el servidor primario, pero se pueden agregar más.

Procedimiento para agregar diversos daemons del repositorio

1. En el menú superior de pdm_edit.pl, seleccione R y pulse la tecla Intro.
Aparecerá el submenú Repository Daemon.
2. Escriba **A** para especificar el nombre de host del servidor.
3. Escriba **primary** para el servidor primario o el nombre del host adecuado si se trata de un servidor secundario.
El daemon de repositorio queda agregado al servidor.

Creación de ejemplos de alias

Los alias son opcionales en CA Service Desk Manager. Este ejemplo explica cómo se prepara la creación de alias y cómo se crean los alias.

Ejemplo: preparación para crear un alias

Antes de poder crear un alias, realice lo siguiente:

1. Defina gestores de objetos y agréguelos a algunos grupos. Los nombres de los gestores de objetos son: domsrvr:group1:11, domsrvr, domsrvr:seattle:12, domsrvr;seattle:13, domsrvr:Tacoma:11.
2. Defina motores Web y asigne gestores de objetos a esos motores Web. Si acepta el valor predeterminado, al gestor de objetos se le asigna domsrvr.
3. Introduzca una expresión regular que coincida con un grupo de gestores de objetos. Si el motor Web conecta a cualquier gestor de objetos, introduzca ANY. Así pues, ANY es el alias predeterminado. Los motores Web y los clientes Java utilizan los alias para especificar ANY o un subconjunto de los gestores de objetos que se están ejecutando a los que se pueden conectar. Por ejemplo, si desea que los clientes Java ubicados en Washington se conecten a los gestores de objetos ubicados en Seattle, hay que conectarlos a /domsrvr:seattle.*. De forma alternativa, puede definir un alias llamado SEATTLE y asignarle el valor /domsrvr:seattle.*.

Ejemplo: creación de un alias

Este ejemplo asume que se ha definido un gestor de objetos y se ha asociado a un grupo denominado Seattle. Si no fuera así, el alias se crea pero se muestra una advertencia. Esta advertencia indica que el alias definido no coincide con ningún gestor de objetos existente.

1. En el menú superior de pdm_edit.pl, seleccione A y pulse la tecla Intro.
Aparecerá el submenú Alias.
2. Escriba el nombre oportuno para el alias; para este ejemplo, escriba **SEATTLE**.
El sistema solicita la expresión regular que se va a asociar con este alias.
3. Escriba **/domsrvr:seattle.***. Esta expresión coincide con todos los gestores de objetos cuyo nombre comience por domsrvr:seattle. Puede usar este alias para la configuración de motores Web y clientes Java.
4. Guarde y salga de la utilidad pdm_edit.pl.
Se crea un script de instalación de alias (llamado alias_install.bat o alias_install.sh).
5. Ejecute el script de instalación de alias en el servidor primario. Esto crea los alias y los transmite a todos los clientes Java y servidores secundarios.

Movimiento de demonios de conocimientos

Los daemon de conocimiento proporcionan la base de conocimiento para CA Service Desk Manager. Se instalan en el servidor primario de forma predeterminada, pero se puede emplear la utilidad `pdm_edit.pl` para moverlos a los servidores secundarios.

Procedimiento para mover daemon de conocimiento

1. En el menú superior de `pdm_edit.pl`, seleccione **K** y pulse la tecla Intro. Aparecerá el submenú Daemon de conocimiento.
2. Introduzca **E** para cambiar el host.
3. Introduzca **primary** para el servidor primario o el nombre adecuado si se trata de un servidor secundario.

Los daemon de conocimiento quedan movidos.

Consideraciones sobre la instalación de personalizaciones

Considere lo siguiente cuando vaya a instalar personalizaciones:

- `pdm_edit.pl` crea un archivo `pdm_startup.dat`. Conserve este archivo para poder editar las opciones seleccionadas.
- `pdm_edit.pl` crea un archivo `pdm_startup.rmt`. Este archivo reemplaza al archivo `pdm_startup.tpl` del directorio `$NX_ROOT/pdmconf` del servidor primario.
- Si emplea un servidor de servlet como Tomcat, la interfaz CGI se reemplaza por un servlet. Estos servidores necesitan un archivo `web.xml.tpl`. La utilidad `pdm_edit.pl` crea un archivo `<nombredehost>-web.xml.tpl` para cada servidor Web. Emplee el archivo apropiado para sustituir el archivo `web.xml.tpl` del directorio `$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF` correspondiente a cada uno de los servidores servlet.
- Si emplea un servidor HTTP como IIS o Apache, debe crear ejecutables de interfaz CGI en el directorio `NX_ROOT/bopcfg/www/wwwroot`. Para hacerlo, copie el archivo `pdmweb.exe` y, a continuación, cambie el nombre. Siga este procedimiento con todas las interfaces CGI de motores Web y WebDirector que haya en los servidores que alojen algún servicio Web.
- Cada motor Web necesita su propio archivo `web.cfg`. `pdm_edit.pl` muestra una lista de los archivos `web.cfg` y los nombres que se van a usar para guardarlos en el servidor apropiado. Por ejemplo, en el servidor primario, hay seis de estos archivos. Llame a un archivo `web.cfg` y a otro `primary-web2.cfg`. La utilidad `pdm_edit.pl` crea archivos `web.cfg` de muestra para cada uno de los motores Web. Cópielos en el directorio `$NX_ROOT/bopcfg/www` del servidor adecuado.

- Si utiliza IIS y necesita agregar extensiones de servidor para las interfaces CGI, `pdm_edit.pl` crea archivos `<nombredehost>-site.dat`. Cópielos en los servidores oportunos y cambie su nombre a `site.dat` en el directorio `$NX_ROOT/bopcfg/www`.
- Si se han definido alias, ejecute el archivo `alias_install.sh` o el archivo `alias_install.bat` en el servidor primario.
- Vuelva a configurar todos los servidores secundarios.
- Vuelva a configurar el servidor primario sin reiniciar la base de datos.

Guardado y salida de `pdm_edit.pl`

Puede guardar los cambios de `pdm_edit.pl` y salir de la utilidad.

Procedimiento para guardar y salir de `pdm_edit.pl`

1. En el menú superior de `pdm_edit.pl`, seleccione `x` y pulse la tecla Intro.
Se le pedirá que seleccione un archivo de plantillas. Este archivo de plantillas sirve como modelo para los archivos `web.cfg` que se crean automáticamente para los motores Web.
2. Seleccione uno de los valores que se muestran. Por ejemplo, seleccione `2` para elegir el archivo `web.cfg.tpl` que está actualmente en uso en el servidor primario. Este procedimiento ayuda a garantizar que las personalizaciones instaladas en el sistema se incluyan en los nuevos archivos `web.cfg.tpl` de ejemplo.
3. Pulse la tecla Intro.
Se guardan los cambios y aparece el símbolo del sistema.

Inicio de WebDirector

WebDirector se puede iniciar en la línea de comandos; o bien, se puede configurar el archivo `pdm_startup` para que WebDirector se inicie automáticamente.

Procedimiento para iniciar WebDirector

1. Abra un símbolo del sistema.
2. Introduzca el siguiente comando:

```
webdirector [-s nombre_s] [-c cgi]
```

3. Utilice las variables de la siguiente manera:

nombre_slump

Especifica el nombre de slump de WebDirector. El nombre de slump identifica de forma exclusiva el proceso de WebDirector. Este argumento sólo es necesario si quiere iniciar más de un WebDirector. De lo contrario, se recomienda dejar el valor predeterminado (web:director).

Cgi

(Opcional) Especifica el nombre del proceso CGI utilizado para WebDirector. Si este argumento no se especifica, se utiliza el predeterminado: pdmweb_d1.exe.

WebDirector se inicia y envía un mensaje a todos los motores Web en ejecución. Los motores Web asociados con ese WebDirector (es decir, los configurados como UseDirector Yes, AfterLogin o BeforeLogin y WebDirectorSlumpName equivalen al nombre de slump de WebDirector) responden con sus parámetros de configuración. Cuando se inicia un motor Web que está configurado para utilizar WebDirector, el motor Web envía sus parámetros de configuración a su WebDirector asociado. Esta acción permite a WebDirector mantener una lista actualizada de todos los motores Web activos.

Cómo gestiona WebDirector las sesiones de usuario

Puede permitir que los usuarios utilicen la URL de cualquier motor Web o la de WebDirector para acceder a CA Service Desk Manager.

Nota: Si todos los motores Web asociados a un WebDirector concreto están configurados con el parámetro UseDirector Yes (es decir, todos los que no usan AfterLogin ni BeforeLogin), el WebDirector funciona estrictamente como equilibrador de carga.

WebDirector gestiona las sesiones de usuario de la siguiente manera:

1. La URL siguiente de WebDirector se publica para los usuarios:
windows y UNIX: `http://hostname/CAisd/pdmweb_d1.exe`
2. Cuando un WebDirector recibe una solicitud, hace lo siguiente para el motor Web:
 - a. Determina si es el más adecuado para gestionar la solicitud.
 - b. Examina el recuento de sesiones actual.
 - c. Calcula la disposición actual mediante la fórmula siguiente:
$$\text{disposición actual} = (\text{disposición configurada}) / (\text{recuento de sesiones} + 1)$$

3. WebDirector redirecciona la solicitud al motor Web con la disposición actual más alta.
4. El motor Web elegido se ocupa de toda la sesión, desde el inicio hasta el cierre.

Si algún usuario del entorno intenta acceder a un motor Web directamente por medio de su propia dirección URL, dicho motor Web envía un mensaje al WebDirector para pedir el redireccionamiento. En caso de que el WebDirector responda con la dirección URL de otro motor, el motor Web original redirige la sesión al motor recomendado.

Cómo se configura WebDirector en un entorno SSL

Considere la información siguiente si uno o más de los motores Web asociados a un WebDirector están configurados con el parámetro UseDirector AfterLogin y el resto de ellos, con el parámetro UseDirector BeforeLogin:

- **UseDirector AfterLogin:** cada vez que WebDirector recibe alguna solicitud, determina el motor Web idóneo para gestionarla, pero sólo opta por los que tienen el parámetro UseDirector AfterLogin. Para el inicio de las sesiones, el WebDirector tiene en cuenta los motores Web cuya disposición es cero. Cuando algún motor Web configurado con el parámetro UseDirector AfterLogin recibe una solicitud (ya sea por redireccionamiento desde otro motor Web, ya porque un usuario accede directamente a su dirección URL), autentica el usuario por el método configurado en el tipo de acceso del usuario. Una vez realizada la autenticación, el motor Web solicita al WebDirector un redireccionamiento. Éste vuelve a elegir otro motor Web de entre todos los que tiene asociados y configurados con el parámetro UseDirector BeforeLogin (salvo los motores cuya disposición es cero). En cuanto el motor Web de autenticación recibe la referencia, transfiere la sesión al motor Web recomendado.
- **UseDirector BeforeLogin:** si algún usuario del entorno intenta acceder de forma directa a un motor Web configurado con el parámetro UseDirector BeforeLogin, éste envía un mensaje al WebDirector para pedir el redireccionamiento. El WebDirector responde con un redireccionamiento a otro motor configurado con el parámetro UseDirector AfterLogin y el motor Web original transfiere la solicitud al motor Web recomendado.

Para configurar WebDirector en un entorno SSL, es recomendable configurar un servidor HTTP para sockets seguros y asociar un solo motor Web a dicho servidor de la siguiente manera:

1. Lea y comprenda cómo WebDirector gestiona las sesiones (see page 398).
2. Configure ese único motor Web con los parámetros UseDirector AfterLogin y WillingnessValue 0.

3. Configure uno o más motores Web para establecer la conexión con un segundo servidor HTTP que use el protocolo HTTP estándar.
4. Configure estos motores Web con los parámetros UseDirector BeforeLogin y WillingnessValue correspondientes según la capacidad relativa de los equipos host.

Así, WebDirector puede dirigir todos los inicios de sesión al servidor seguro (ya que los servidores sin disposición siguen siendo aptos para el inicio de sesión) y remite a los demás motores Web para el resto de las sesiones.

Mejora del funcionamiento con el almacenamiento en caché de los exploradores

La interfaz Web de CA Service Desk Manager usa mucho código JavaScript, muchas hojas de estilo y muchos archivos de imágenes, que pueden llegar a alcanzar un tamaño considerable y afectar el rendimiento.

Para mejorar el rendimiento de la interfaz Web, configure el servidor HTTP de forma que el navegador del usuario almacene en caché estos archivos para hacer que se carguen una sola vez al día.

El rendimiento de la interfaz Web mejora.

Nota: La instalación predeterminada configura de manera automática el almacenamiento en caché en el caso de servidores Apache e IIS. Sin embargo, se puede configurar de forma manual.

Configuración de Microsoft Internet Information Server

Puede configurar Microsoft Internet Information Server (IIS) para que notifique al explorador que los archivos cargados del directorio de CA Service Desk Manager caducan un día después de haberse cargado. Eso significa que el explorador realiza una consulta al servidor sobre dichos archivos sólo una vez al día, independientemente de la cantidad de veces que se utilicen.

Procedimiento para configurar Microsoft Internet Information Server

1. Inicie la aplicación Administrador de servicios de Internet (en Windows 2000 y XP, seleccione Programas/Todos los programas > Herramientas administrativas > Administrador de servicios de Internet).
2. Acceda a la carpeta de archivos de CA Service Desk Manager, cuyo nombre suele ser CAisd.
 - a. Haga clic en el signo más ubicado junto al servidor donde se ejecuta la interfaz Web de CA Service Desk Manager.
 - b. Haga clic en el signo más ubicado junto al sitio Web predeterminado.
 - c. Desplácese hasta CAisd.
3. Haga clic con el botón secundario en la carpeta CAisd y seleccione Propiedades.

Aparecerá la página Propiedades.
4. Acceda a la ficha Encabezados HTTP.
5. Seleccione la casilla de verificación Habilitar caducidad de contenido.
6. Seleccione la opción Caducar después de, escriba 1 en el campo de texto y seleccione un día en la lista desplegable.
7. Haga clic en OK.

Las propiedades se guardan y los cambios se aplican inmediatamente.

Configuración de Apache

Es posible configurar Apache para que notifique al explorador que los archivos cargados del directorio de CA Service Desk Manager caducan un día después de la carga. Esta configuración significa que el explorador realiza una consulta al servidor sobre dichos archivos sólo una vez al día, independientemente del número de veces que se utilicen.

Apache se configura modificando un archivo de configuración de texto. La instalación predeterminada modifica el archivo de configuración activo en el directorio conf de Apache (normalmente httpd.conf) que va a contener la instrucción:

```
Include directorio-instalación/bopcfg/www/CAisd_apache.conf
```

Directorio de instalación debe ser reemplazado con una ruta completa. En Windows, la ruta suele ser c:\Archivos de programa\CA\CA Service Desk Manager. En UNIX, sustituya el *directorio-instalación* por el valor de \$NX_ROOT.

El archivo CAisd_apache.conf, al que se hace referencia mediante la instrucción Include, contiene el texto siguiente. De nuevo, el *directorio de instalación* se reemplaza con la ruta completa como estaba en la instrucción Include.

```
<IfModule mod_alias.c>
    Alias /CAisd directorio-instalación/bopcfg/www/wwwroot/
    <IfModule mod_expires.c>
        <Directory directorio-instalación/bopcfg/www/wwwroot>
            ExpiresActive    On
            ExpiresDefault   "access plus 1 day"
        </Directory>
    </IfModule>
</IfModule>
```

Si desea configurar Apache de forma manual para que se almacenen en la caché del explorador los archivos de CA Service Desk Manager, incluya instrucciones parecidas a las del archivo CAisd_apache.conf en el archivo de configuración de Apache. Puede optar por agregarlas directamente al archivo o por agregar una instrucción Include que haga referencia a otro archivo, como se hace en la instalación predeterminada.

Los cambios efectuados en los archivos de configuración de Apache se aplican sólo después de haber reiniciado el servidor.

Borrado de cachés

Si modifica un archivo de JavaScript, una imagen, una hoja de estilo, un archivo HTML o un archivo de ayuda que el servidor HTTP mismo ha cargado, debe recomendar a los usuarios borrar la memoria caché del explorador.

Nota: Para que se apliquen los cambios de los archivos HTML, debe reciclar el motor Web o utilizar la utilidad pdm_webcache. En un entorno de desarrollo, es posible saltarse este requisito si se especifica la propiedad SuppressHtmlCache del archivo de configuración.

Procedimiento para borrar la memoria caché de Internet Explorer

1. Seleccione Herramientas, Opciones de Internet.
Aparecerá el cuadro de diálogo Opciones de Internet.
2. Haga clic en Eliminar archivos.
Aparecerá una ventana de confirmación.
3. Haga clic en OK.
Se ha borrado la memoria caché del explorador.

Procedimiento para borrar la memoria caché de Firefox

1. Seleccione Herramientas, Borrar área privada.
2. Haga clic en el botón Borrar datos privados ahora.

Se ha borrado la memoria caché del explorador.

Comportamiento de bloqueo de registros en la interfaz Web

Cuando los usuarios editan registros de la base de datos mediante la interfaz Web, se les otorga un bloqueo exclusivo para los registros durante dos minutos, que es el tiempo predeterminado. Puede modificar el tiempo predeterminado mediante la propiedad `ExclLockSeconds` del archivo `web.cfg`.

Las condiciones que se describen a continuación determinan si un registro de la base de datos se actualiza o no con los cambios de un usuario:

- Si un usuario *puede* editar y enviar cambios dentro de un tiempo asignado, los cambios se incluyen en la base de datos.

Durante el tiempo que permanecen bloqueados los registros de la base de datos, los demás usuarios (Web y otros) pueden consultarlos pero no pueden editarlos. Si algún otro usuario intenta editar un registro mientras está bloqueado, aparece un mensaje de error.

- Si un usuario *no puede* editar ni enviar cambios dentro de un tiempo asignado, el bloqueo del registro se anula automáticamente y otros usuarios pueden editar el registro.

Cuando el usuario envía las actualizaciones, se comprueban las marcas de tiempo para garantizar que nadie más haya modificado el registro y ocurre lo siguiente:

- Si el registro no ha sufrido ningún otro cambio desde la anulación del bloqueo exclusivo, se guardan las modificaciones del usuario en la base de datos.
- En caso de que otro usuario haya editado el registro tras el vencimiento del bloqueo, aparece una respuesta de error cuando el usuario trata de guardar el registro y no se registran los cambios. El usuario debe reiniciar el proceso de edición y volver a introducir los cambios.

Más información:

[Modificación del archivo de configuración](#) (en la página 404)

Impresión de páginas Web de CA Service Desk Manager

CA Service Desk Manager utiliza imágenes de fondo para dar formato a los botones y a las fichas de los blocs de notas. El valor predeterminado de numerosos exploradores indica que *no* se impriman dichas imágenes. Por ello, al elegir Archivo > Imprimir en la barra de menús del explorador o en el menú de CA Service Desk Manager, la página impresa tan sólo muestra las esquinas de los botones y las fichas.

Procedimiento para imprimir páginas Web de CA Service Desk Manager en Internet Explorer

1. Seleccione Herramientas, Opciones de Internet.
Aparecerá el cuadro de diálogo Opciones de Internet.
2. Seleccione la ficha Avanzadas.
3. Desplácese hasta el encabezado Impresión y seleccione la opción Imprimir colores e imágenes de fondo.

Las páginas Web impresas de CA Service Desk Manager incluyen gráficos de fondo.

Procedimiento para imprimir páginas Web de CA Service Desk Manager en Firefox

1. Seleccione Archivo, Configurar página.
2. Seleccione la ficha Formato y opciones.
3. Seleccione la casilla de verificación Imprimir fondo (colores e imágenes).

Las páginas Web impresas de CA Service Desk Manager incluyen gráficos de fondo.

Modificación del archivo de configuración

Al instalar la interfaz Web de CA Service Desk Manager, se instala un archivo web.cfg de muestra en el directorio \$NX_ROOT/bopcfg/www, el cual se puede modificar según las necesidades. El propio archivo web.cfg contiene información útil en forma de comentarios que se puede leer al abrir el archivo.

Nota: Algunas otras variables de configuración, como la de conjunto de caracteres, también se encuentran disponibles en el Gestor de opciones. Para acceder a estas variables, se puede utilizar la ficha Administración de la interfaz Web. Para obtener más información al respecto, consulte la *ayuda en línea*.

AllowInactiveSrelEntry

Especifica si se puede o no guardar un registro que hace referencia a registros inactivos de tablas de referencia.

- Si se omite esta propiedad o se define en 0, las entradas de las tablas de referencia (por ejemplo, estado de solicitud o categoría de cambio) que estén inactivas no se incluyen en las listas de selección desplegables ni tampoco se pueden especificar en las búsquedas o en los campos de búsqueda jerárquica.
- Si se define en 1, se ignora el indicador de inactividad en las entradas de las tablas de referencias.

Sea cual sea el valor de este indicador, sí se pueden guardar los registros que ya contuvieran una referencia a alguna entrada inactiva de una tabla de referencias sin necesidad de cambiar dicha referencia; el indicador sólo afecta a los nuevos valores de los campos.

AnnouncementLength

Especifica el número máximo de anuncios que se muestran en la pantalla de apertura de la interfaz de clientes y analistas. CA Service Desk Manager muestra primero el anuncio más reciente y continúa mostrando la cantidad de anuncios que este parámetro especifica. Los usuarios de la interfaz de analistas pueden ver más anuncios al seleccionar Anuncios en el menú Buscar.

Valor predeterminado: 10, lo cual significa que se muestran los diez anuncios más recientes.

AnonymousPrio

Especifica las prioridades válidas para los tickets creados por usuarios invitados. es decir, estos usuarios sólo pueden especificar en sus partes una de las prioridades presentes en la lista de la propiedad AnonymousPrio. Las entradas de la lista de prioridades se separan por espacios. Las entradas pueden ser un número del 1 al 5 o la palabra "ninguno". La prioridad predeterminada de los partes creados por los usuarios invitados se especifica en primer lugar y puede aparecer repetida en la lista.

Los valores válidos para la propiedad AnonymousPrio se corresponden con los nombres simbólicos iniciales de las prioridades, aunque estos nombres se pueden personalizar con los clientes Java. Ello, no obstante, no afecta a la especificación de la propiedad AnonymousPrio, que sigue haciendo referencia a las prioridades por sus nombres predeterminados de forma que 1, por ejemplo, corresponde a la máxima prioridad.

Valor predeterminado: Ninguno, lo cual significa que las solicitudes creadas por los usuarios invitados no tienen ninguna prioridad.

Relleno automático

Especifica que la interfaz Web debe rellenar de forma automática los campos de búsqueda cuando los usuarios escriben datos dentro de ellos y pulsan la tecla de tabulación para salir del campo. Al hacer esto, si la opción Relleno automático está seleccionada, el explorador pide al servidor que confirme si la modificación es correcta. Como resultado, se rellena el campo con el nombre completo (si el usuario ha proporcionado parte del nombre) o aparece una ventana de búsqueda (si la selección del usuario es incorrecta o ambigua).

Esta propiedad es opcional. De forma predeterminada, la propiedad Relleno automático está activada; por lo tanto, si se omite su ID o se establece en Sí, al salir de un campo de búsqueda con la tecla de tabulación, se inicia automáticamente una búsqueda en la base de datos. Si esta propiedad se establece en No, los campos de búsqueda no se rellenan automáticamente ni se verifican hasta que se intenta guardar el registro.

CAisd

Especifica la ruta (incluida una barra al principio) al alias o al directorio virtual del servidor HTTP que alberga los archivos que necesita el servidor Web de CA Service Desk Manager. Por lo general, esta propiedad dispone del valor /CAisd tanto en las instalaciones de UNIX como en las de Windows. En el caso de los servidores Apache, se debe definir en una instrucción Alias en el archivo de configuración. En el caso de IIS, debe coincidir con el campo Alias de la ventana Propiedades de directorio.

CGI

Especifica el nombre del programa ejecutable de CGI que se suministra con la interfaz Web (sin la extensión .exe).

Valor predeterminado: pdmweb

Nota: Si cambia el nombre del programa, debe actualizar esta propiedad.

CgiReport

Especifica el nombre del programa ejecutable de CGI para informes Web que se suministra con la interfaz Web (sin la extensión .exe).

Valor predeterminado: pdm_cgireport

Nota: Si cambia el nombre del programa, debe actualizar esta propiedad.

ContactAutoDesc

Especifica si se debe insertar el nombre de un contacto en la descripción de las incidencias y las solicitudes nuevas creadas en las interfaces de clientes y empleados. Si se omite la propiedad o se define en 0, no se agrega ninguna información automática a dicha descripción. Ahora bien, si se especifica 1, se inserta de forma automática el nombre de los contactos en la descripción de las incidencias y las solicitudes nuevas que se creen en las interfaces de clientes y empleados. Esta propiedad no tiene ningún efecto en la interfaz de los analistas.

ContactAutoDescWithIP

Especifica si se debe insertar la dirección IP de un contacto en la descripción de las incidencias y las solicitudes nuevas creadas en las interfaces de clientes y empleados. Si se omite la propiedad o se define en 0, no se agrega ninguna información de dirección IP a dicha descripción. Ahora bien, si se especifica 1 tanto en esta propiedad como en la propiedad ContactAutoDesc, se insertan de forma automática el nombre y la dirección IP de los contactos en la descripción de las incidencias y las solicitudes nuevas que se creen en las interfaces de clientes y empleados. Esta propiedad no tiene ningún efecto en la interfaz de los analistas. Se omite a menos que la propiedad ContactAutoDesc se haya definido en 1.

CstPrio

Especifica prioridades válidas para las incidencias creadas con la interfaz Web de los clientes. Los usuarios de esta interfaz sólo pueden especificar en sus incidencias una de las prioridades presentes en la lista de la propiedad CstPrio y no pueden actualizar dicha prioridad en caso de que algún analista la haya cambiado a otra que no figure en la lista.

Las entradas de la lista de prioridades se separan por espacios. Las entradas pueden ser un número del 1 al 5 o la palabra "ninguno". La prioridad predeterminada de las incidencias creadas en la interfaz de clientes se especifica en primer lugar y puede aparecer repetida en la lista.

Valor predeterminado: ninguno, 3, 4, 5

Los valores válidos para la propiedad CstPrio se corresponden con los nombres simbólicos iniciales de las prioridades, aunque estos nombres se pueden personalizar con los clientes Java. Ello, no obstante, no afecta a la especificación de la propiedad CstPrio, que sigue haciendo referencia a las prioridades por sus nombres predeterminados de forma que 1, por ejemplo, corresponde a la máxima prioridad.

DateFormat

Especifica el orden de los elementos de las fechas.

Valor predeterminado: MM/DD/YYYY hh:mm:ss (a.m./p.m.)

Símbolo	Descripción
M	Imprime 1 dígito o 2 del mes
MM	Imprime 2 dígitos del mes
S	Imprime 1 dígito o 2 del día
DD	Imprime 2 dígitos del día
YY	Imprime 2 dígitos del año
YYYY	Imprime 4 dígitos del año
A	Imprime 1 dígito o 2 de la hora en formato de 24 horas
HH	Imprime 2 dígitos de la hora en formato de 24 horas
A	Imprime 1 dígito o 2 de la hora en formato de 12 horas
hh	Imprime 2 dígitos de la hora en formato de 12 horas
M	Imprime 1 dígito o 2 de los minutos
mm	Imprime 2 dígitos de los minutos
S	Imprime 1 dígito o 2 de los segundos
ss	Imprime 2 dígitos de los segundos
a(a. m., p. m.)	Imprime a. m. y p. m. como cadena

DateFormatNoTime

Especifica la misma definición que la propiedad DateFormat pero sin especificar la hora.

DebugSource

Habilita el menú contextual estándar del explorador en los formularios de CA Service Desk Manager. Si no se define esta propiedad, al hacer clic con el botón secundario en un formulario, se abre un menú de CA Service Desk Manager. Esta propiedad se debe configurar con sumo cuidado, ya que algunas de las opciones del menú contextual estándar del explorador pueden provocar errores de ejecución (ésta es la razón por la cual suele estar desactivada). En Internet Explorer, se puede acceder al menú contextual estándar del explorador aunque no se haya definido la propiedad DebugSource si se pulsa y se mantiene pulsada la tecla Ctrl al hacer clic con el botón derecho.

DebugTrace

Hace que el motor Web escriba información de seguimiento en el archivo stdlog.

Importante: esta propiedad *no* se debe establecer para uso común. Se debe utilizar solamente cuando el personal de soporte técnico de CA lo solicita.

EmpPrio

Especifica prioridades válidas para las solicitudes creadas con la interfaz Web de los empleados. Los usuarios de esta interfaz sólo pueden especificar en sus solicitudes una de las prioridades presentes en la lista de la propiedad EmpPrio y no pueden actualizar dicha prioridad en caso de que algún analista la haya cambiado a otra que no figure en la lista.

Las entradas de la lista de prioridades se separan por espacios. Las entradas pueden ser un número del 1 al 5 o la palabra "ninguno". La prioridad predeterminada de las solicitudes creadas en la interfaz de empleados se especifica en primer lugar y puede aparecer repetida en la lista.

Valor predeterminado: ninguno, 3, 4, 5

Los valores válidos para la propiedad EmpPrio se corresponden con los nombres simbólicos iniciales de las prioridades, aunque estos nombres se pueden personalizar con los clientes Java. Ello, no obstante, no afecta a la especificación de la propiedad EmpPrio, que sigue haciendo referencia a las prioridades por sus nombres predeterminados de forma que 1, por ejemplo, corresponde a la máxima prioridad.

ExclLockSeconds

Especifica el número máximo de segundos durante el que se otorga a los usuarios un bloqueo exclusivo en un registro después de hacer clic en Editar. Cuando transcurre ese plazo, el motor Web anula el bloqueo y permite la actualización del registro por parte de otros usuarios. El motor Web intenta retomar el bloqueo si el usuario solicita guardar los cambios tras haber vencido el valor de ExclLockSeconds. Este intento sólo llega a buen término si ningún otro usuario ha actualizado el registro mientras estaba disponible el bloqueo. En caso contrario, el primer usuario debe volver a especificar las modificaciones.

Valor predeterminado: 120 (dos minutos)

Este argumento es opcional. Si se omite, se asume el valor predeterminado.

Nota: El valor de la propiedad ExclLockSeconds debe ser inferior al valor de la propiedad Timeout. La propiedad ExclLockSeconds se especifica en segundos mientras que la propiedad Timeout se especifica en minutos.

FormCacheMax

Especifica el número máximo de formularios que se conserva en la memoria del motor Web para cada usuario. El motor Web siempre mantiene los últimos formularios de FormCacheMax que hayan empleado los usuarios. Los formularios que superen este número pueden sufrir un agotamiento del tiempo de espera. Si eso sucede, no es posible acceder a dichos formularios mediante los botones de acceso a las páginas anterior y siguiente de la página principal ni tampoco se pueden enviar si se trata de formularios emergentes.

Valor predeterminado: 10

Los formularios cuyo tiempo de espera se ha agotado ahorran espacio en la memoria del motor Web pero, en ocasiones, es necesario que los usuarios los actualicen de forma manual. Para desactivar la función FormTimeout, puede definir la propiedad FormCacheMax en -1.

FormTimeout

Especifica el número mínimo de segundos durante el que se conservan los formularios en los motores Web antes de que sean aptos para su eliminación de la memoria caché. Los usuarios siempre tienen por lo menos el número de segundos especificado en este parámetro para trabajar en un formulario antes de enviarlo. Además, el motor Web siempre mantiene los últimos formularios de FormCacheMax que hayan empleado los usuarios.

La propiedad StayCacheList permite impedir que determinados formularios superen el tiempo de espera.

Valor predeterminado: 180 (3 minutos)

FormTitle

Especifica la cadena que se debe incluir en la barra de título del explorador Web al mostrar formularios Web de CA Service Desk Manager. El valor de la propiedad FormTitle complementa el título del formulario que se haya abierto.

Valor predeterminado: CA Service Desk Manager

Por ejemplo, si se conserva el valor predeterminado y se utiliza Microsoft Internet Explorer para mostrar el formulario Detalles de anuncio, la barra del título presenta lo siguiente:

"Detalles de anuncio-CA Service Desk Manager-Microsoft Internet Explorer".

Esta propiedad es opcional. Si se omite, la interfaz Web de los analistas no usa ningún valor constante en el título. Las interfaces Web de clientes y PDA se revierten al valor predeterminado.

HitTrackFile

Especifica la ruta completa al archivo donde se registran todas las páginas Web utilizadas. En este archivo se escribe una línea cada vez que los usuarios solicitan una página. El archivo puede crecer indefinidamente, así que se debe prestar atención al usar esta propiedad.

Nota: Los registros que contengan una indicación de tiempo, un ID de usuario, un ID de registro de la base de datos y el nombre de un formulario HTML se agregan a este archivo. El formato de los registros puede cambiar. Es preciso realizar un mantenimiento de este archivo cada cierto tiempo para que no llegue a ser demasiado grande.

Esta propiedad es opcional. Si se omite, no se escribe ningún archivo de seguimiento de coincidencias.

HtmlCacheSize

Especifica el tamaño de la memoria caché HTML. Si se supera este tamaño, se elimina de la memoria caché el formulario menos utilizado.

Valor predeterminado: 1000.

ListAllMaximum

Especifica el número máximo de registros que puede mostrarse en las listas antes de que una petición para mostrar la lista completa haga que aparezca un mensaje de aviso emergente para advertir al usuario de que la petición tiene un impacto negativo en el rendimiento, por lo que no se permite.

Valor predeterminado: 2500

ListAllWarn

Especifica el número máximo de registros que puede mostrarse en las listas antes de que una petición para mostrar la lista completa haga que aparezca un mensaje de aviso emergente para advertir al usuario de que la petición puede tener un impacto negativo en el rendimiento, por lo que se solicita confirmación.

Valor predeterminado: 1000

ListBottomMaximum

Especifica el número máximo de registros que puede mostrarse en las listas antes de que una petición para desplazarse al final de la lista haga que aparezca un mensaje de aviso emergente para advertir al usuario de que la petición tiene un impacto negativo en el rendimiento, por lo que no se permite.

Valor predeterminado: 2500

ListBottomWarn

Especifica el número máximo de registros que puede mostrarse en las listas antes de que una petición para desplazarse al final de la lista haga que aparezca un mensaje de aviso emergente para advertir al usuario de que la petición puede tener un impacto negativo en el rendimiento, por lo que se solicita confirmación.

Valor predeterminado: 1000

ListPageLength

Especifica el número máximo de registros encontrados que se debe mostrar en una página de lista tras realizar alguna búsqueda.

Valor predeterminado: 10

LogoutURL

Especifica la URL completa de una página Web que aparece cuando los usuarios cierran una sesión de CA Service Desk Manager. Esta propiedad es opcional. Si no se especifica, vuelve a aparecer el formulario de inicio de sesión.

Lr_Refresh

Especifica el intervalo de actualización del lector de registro en segundos. Si la propiedad tiene otro valor que no sea cero, el lector del registro de notificaciones se actualiza automáticamente según el intervalo indicado (como mínimo, de treinta segundos).

Esta propiedad es opcional. Si se omite, se actualiza cada cinco minutos, ya que el valor predeterminado es 300 segundos. En caso de que se defina en cero, el lector no se actualiza nunca.

MacroPath

Especifica la lista de rutas de directorio en las que los motores Web buscan los archivos que solicita la etiqueta PDM_MACRO. Cabe la posibilidad de especificar varios directorios separados por espacios. Si se desea, existe la opción de incluir variables de entorno en los nombres de los directorios; para ello, basta con anteponer el símbolo del dólar (por ejemplo, \$NX_ROOT). Tanto en Windows como en UNIX, los componentes de las rutas se separan con barras normales (/), no inversas (\). Esta propiedad es obligatoria. Se suele definir de la siguiente manera:

```
$NX_ROOT/site/mods/macro $NX_ROOT/bopcfg/www/macro
```

MatchesFound

Especifica el texto de los mensajes que se muestran bajo los campos cuando la entrada del usuario en los campos de búsqueda es ambigua y se debe volver a mostrar el formulario de edición con una lista de selección desplegable. Esta propiedad es opcional. Si se omite, adopta el valor predeterminado "Varias coincidencias".

MaxSelectList

Especifica el número máximo de coincidencias que se muestra en la lista de selección desplegable que aparece cuando la entrada del usuario en los campos de búsqueda es ambigua y se debe volver a mostrar el formulario de edición. Si se encuentran más coincidencias de las especificadas, se muestra el mensaje indicado para Demasiadas coincidencias.

NoMatchesFound

Especifica el texto de los mensajes que se muestran bajo los campos cuando la entrada del usuario en los campos de búsqueda es incorrecta y se debe volver a mostrar el formulario de edición. Esta propiedad es opcional. Si se omite, adopta el valor predeterminado "No se han encontrado coincidencias".

PreLogin Timeout

Especifica el número máximo de minutos que el motor Web mantiene activas las sesiones antes de que se produzca algún inicio de sesión. Los motores Web inician de forma automática una sesión cuando los usuarios solicitan el formulario de inicio de sesión, antes incluso de que rellenen los datos pertinentes. Si no se indican esos datos dentro del período indicado en esta propiedad, el motor Web destruye la sesión. Si, después, el usuario inicia una sesión, el motor Web crea otra sesión sin que lo advierta el usuario.

Esta propiedad no tiene ningún impacto en el usuario final. Su único fin tiene que ver con el rendimiento: equilibrar el uso de la memoria de los motores Web frente a la sobrecarga que supone destruir y volver a crear las sesiones. Esta propiedad es opcional. Si se omite, adopta el valor predeterminado de un minuto.

RedirectingURL

Especifica la dirección URL que debe usar WebDirector para enviar las peticiones al motor Web oportuno. Se indica la dirección URL completa del motor, incluido el protocolo http. Esta propiedad es obligatoria si se utiliza WebDirector; en caso contrario, se ignora.

SchedExpMaximum

SchedExpMaximum

Especifica el límite del número de eventos de programación que se pueden exportar a la vez.

Valor predeterminado: 1000

Importante: el valor predeterminado es las exportaciones máximas que CA Service Desk Manager puede ejecutar a la vez. Aumentar el valor predeterminado podría causar inestabilidad del sistema. Si intenta exportar más que el valor especificado en SchedExpMaximum, aparecerá un mensaje en el que se rechaza la solicitud de exportación.

SellistCacheExclude

SellistCacheExclude

Especifica los nombres de las fábricas (objetos) que se han de excluir del almacenamiento en la memoria caché de las listas de <PDM_SELECT>. A fin de mejorar el rendimiento, el motor Web suele almacenar en su propia memoria caché el contenido de las tablas pequeñas utilizadas en las listas (desplegables) de <PDM_SELECT> y las listas de búsqueda jerárquica. Si se emplean restricciones de particiones de datos para especificar las distintas vistas de las tablas que deben ver los diversos usuarios, es conveniente suprimir el almacenamiento en memoria caché de la tabla pertinente. Además, al incluir ciertas tablas en el valor de esta propiedad, el motor Web ya no tiene que consultar el recuento de registros al inicio, lo que mejora ligeramente el rendimiento en esta fase. Esta propiedad es opcional. Si se especifica, debe albergar el nombre de un objeto o los de varios separados por espacios.

SellistCacheMax

SellistCacheMax

Define el número máximo de registros de las tablas que se puede almacenar en la memoria caché de los motores Web. Éstos mantienen todo el contenido de las tablas que coincida con el tamaño de la caché o que esté por debajo de él en su propia memoria, lo que mejora el rendimiento en la creación de listas <PDM_SELECT> que usen estas tablas. Si se indica un valor mayor en esta propiedad, se mejora el rendimiento en detrimento de un mayor uso de la memoria.

Valor predeterminado: 10

La propiedad SellistCacheMax se ignora en las tablas usadas en listas de búsqueda jerárquica, como en el caso de las categorías de las solicitudes, las incidencias y las órdenes de cambios. El motor Web siempre almacena el contenido completo de las tablas empleadas en dichas listas en su propia memoria. Si alguna de ellas cuenta con un número elevado de valores, quizá sea conveniente especificar la propiedad SellistCachePreload.

SellistCachePreload

Especifica al menos una tabla que se carga en la memoria caché de selección de los motores Web en el momento del inicio. Las que no aparezcan en esta propiedad se cargan cuando se haga uso de ellas. Si el valor de SellistCacheMax es elevado o alguna lista de búsqueda jerárquica cuenta con numerosos registros (como las categorías), resulta adecuado especificar la tabla en la propiedad SellistCachePreload. Así se evita el retardo en el tiempo de respuesta la primera vez que se accede a algún formulario que use dicha tabla.

La especificación de la propiedad `SelListCachePreload` consiste en una lista de nombres de objetos separados por espacios. Cada uno de esos nombres puede ir seguido por una lista opcional de nombres de atributos entre paréntesis, que son los atributos que se cargan en el motor Web. Si no se especifica ningún atributo, sólo se cargan el nombre común y el valor del atributo relacionado. Esto es suficiente para las listas de selección desplegables, pero no para las búsquedas jerárquicas. Después de haber modificado los formularios de búsqueda jerárquica (`hierse1_xx.html`, donde `xx` es el nombre de un objeto), asegúrese de que la propiedad `SelListCachePreload` especifique todos los atributos empleados en los formularios. Si se omite alguno de ellos, se vuelve a cargar la caché al usar el formulario.

La propiedad `SelListCachePreload` es opcional. Si se omite, no se carga nada en la caché de selección hasta que algún usuario solicite un formulario mediante una lista de selección desplegable o una búsqueda jerárquica.

```
chgcat(description owning_contract) chgstat crs isscat(description
owning_contract) issstat pcat(description cr_flag in_flag pr_flag
owning_contract) pri tskstat urg pcat_cr(description cr_flag in_flag pr_flag
owning_contract) pcat_pr(description cr_flag in_flag pr_flag owning_contract)
pcat_in(description cr_flag in_flag pr_flag owning_contract)
```

StayCacheList

Especifica los nombres de los formularios que no se eliminan nunca de la memoria caché de formularios, independientemente del tiempo que haga que se mostraron. Esta propiedad garantiza la conservación de los marcos fijos en las presentaciones con marcos a lo largo de toda la sesión. Si se usa con cuidado, sirve para dejar otros formularios almacenados en caché de forma permanente. El valor predeterminado es el siguiente:

```
scoreboard.html top_splash.html buttons.html hierse1_admin_tree.html
```

SuppressHtmlCache

Especifica que los motores Web deben volver a leer todos los archivos que definan el contenido de las páginas cada vez que éstas se soliciten. El análisis de los archivos HTML suele tardar bastante en cuanto a lo que procesamiento del motor Web se refiere y suele implicar la lectura de varios archivos físicos (puesto que la mayoría de las páginas usa etiquetas `PDM_INCLUDE`). Por lo general, el motor Web guarda los archivos analizados en su propia memoria a fin de satisfacer al instante las futuras solicitudes de las mismas páginas. Aunque este comportamiento mejora de forma considerable el rendimiento, resulta algo incómodo para los usuarios que desarrollan páginas nuevas o actualizadas, ya que se debe reiniciar el motor Web para que se apliquen los cambios.

Esta propiedad es opcional y no exige ningún valor. Si se especifica, el motor Web no almacena en caché los archivos analizados y los cambios realizados en los archivos HTML se aplican de inmediato. Dado su impacto en el rendimiento, no conviene especificar esta propiedad en los entornos de producción.

SuppressLoginAndLogoutMsg

Especifica que los motores Web no deben registrar mensajes en el archivo de registro de CA Service Desk Manager cada vez que algún usuario inicie una sesión en la interfaz Web o cierre la sesión abierta.

Esta propiedad es opcional. Si no se especifica, el motor Web registra un mensaje al iniciar una sesión o al cerrar la sesión abierta.

SuppressMacroCache

Especifica que los motores Web deben descartar todas las macros guardadas cada vez que se solicite una nueva página. Por lo general, el motor Web guarda las macros analizadas en su propia memoria a fin de satisfacer al instante las futuras solicitudes de las mismas macros. Aunque este comportamiento mejora el rendimiento, resulta algo incómodo para los usuarios que desarrollan macros nuevas o actualizadas, ya que se debe reiniciar el motor Web para que se apliquen los cambios.

Esta propiedad es opcional. Si se especifica, el motor Web no almacena en caché las macros analizadas y los cambios realizados en las macros se aplican de inmediato. Dado su impacto en el rendimiento, no conviene especificar esta propiedad en los entornos de producción.

tiempo de espera agotado.

Especifica el número de minutos durante los que puede permanecer inactiva la sesión de los usuarios antes de su finalización automática con objeto de liberar todos los recursos del servidor.

Nota: El valor de la propiedad Timeout debe ser más largo que el valor de la propiedad ExclLockSeconds. La propiedad ExclLockSeconds se especifica en segundos mientras que la propiedad Timeout se especifica en minutos.

TooManyMatches

Especifica el texto de los mensajes que se muestran bajo los campos cuando la entrada del usuario en los campos de búsqueda es ambigua y el número de coincidencias supera el valor de la propiedad MaxSelectList. Esta propiedad es opcional. Si se omite, adopta el valor predeterminado de "Demasiadas coincidencias".

UpdatedAnnouncementsPopup

El intervalo en que el explorador comprueba si hay anuncios nuevos. Si se encuentra algún anuncio nuevo, se muestra automáticamente en un cuadro emergente. El valor del intervalo se indica en minutos. Para reducir el impacto en el rendimiento del explorador, se recomienda definir esta variable en un valor superior a 5 (minutos).

UseDirector

Especifica cuándo el WebDirector está controlando este motor Web. En la tabla siguiente se definen los posibles valores:

Valor	Descripción
No	El motor Web es independiente del WebDirector. Se trata del valor predeterminado.
Sí	El WebDirector debe iniciar todas las sesiones, incluido el formulario de inicio de sesión. En caso de que algún usuario intente establecer una conexión directa con un motor Web, éste solicita al WebDirector una referencia.
AfterLogin	El motor Web remite la sesión al WebDirector tras autenticar al usuario. Los motores Web configurados con el parámetro UseDirector AfterLogin sólo son responsables de la autenticación y, por lo tanto, se convierten en candidatos para el uso de sockets seguros (SSL) cuando se pretende lograr la máxima seguridad.
BeforeLogin	El motor Web remite la sesión al WebDirector antes de autenticar al usuario. Los motores Web configurados con el parámetro UseDirectory BeforeLogin no muestran nunca la página de inicio de sesión ni aceptan contraseñas para este fin.

Esta propiedad es opcional. Si se omite, el motor Web no usa el WebDirector.

WebDirectorSlumpName

Especifica el nombre del WebDirector que provee servicio al motor Web oportuno. Sólo es necesaria si se ejecuta más de un WebDirector o si el WebDirector está configurado para emplear un nombre de slump que no sea el predeterminado (web:director).

Esta propiedad es opcional si se utiliza WebDirector; en caso contrario, se ignora.

WillingnessValue

Especifica la disposición de este motor Web de aceptar sesiones, basado en una escala de 0 a 10. Esta propiedad sólo se utiliza si se usa WebDirector. Este valor es significativo tan sólo en comparación con la disposición de otros motores Web asociados al mismo WebDirector. El WebDirector transfiere las sesiones a los motores Web de manera proporcional a sus respectivos valores de disposición. Por ejemplo, los motores Web cuyo valor de disposición duplica el valor de otros motores suelen atender el doble de sesiones.

Si el valor de la propiedad WillingnessValue es cero, significa que el motor Web no acepta ninguna sesión. Este valor resulta útil cuando se define la propiedad UseDirector en el valor AfterLogin.

Esta propiedad es opcional si se utiliza WebDirector; en caso contrario, se ignora. Si se omite, el motor Web define su disposición en 5.

WorkFrameTimeout

Especifica el número máximo de segundos que esperan los motores Web la respuesta a las peticiones de servidores internos antes de llegar a la conclusión de que se trata de peticiones fallidas. El marco de trabajo se emplea en las funciones de la interfaz Web de CA Service Desk Manager que exigen otros datos del servidor aparte de las páginas Web normales, por ejemplo, funciones como el relleno automático, la carga de propiedades de las categorías o la actualización de los recuentos del panel de resultados. No es probable que fallen las solicitudes del marco de trabajo realizadas a CA Service Desk Manager. No obstante, las destinadas a otros servidores (por ejemplo, productos integrados como Gestión del conocimiento) pueden fallar si el servidor pertinente no se está ejecutando o si algún problema de red impide el acceso a él. La propiedad WorkFrameTimeout especifica el plazo que ha de transcurrir para considerar que ha fallado una solicitud y que el marco de trabajo está disponible para otras solicitudes.

Nota: No se comprueba la propiedad WorkFrameTimeout a menos que haga falta algún marco de trabajo y todos los marcos de trabajo estén en uso. Por consiguiente, los servidores remotos suelen tener más tiempo para responder que el especificado en la propiedad WorkFrameTimeout. El valor de WorkFrameTimeout es el mínimo.

Esta propiedad es opcional. Si se omite, el motor Web aplica 30 segundos como tiempo de espera del marco de trabajo.

Capítulo 10: Configuración de la asignación automática

Esta sección contiene los siguientes temas:

[Asignación automática](#) (en la página 419)
[Relaciones de asignación automática](#) (en la página 420)
[Métodos de asignación automática](#) (en la página 420)
[Cómo empezar a implementar la asignación automática](#) (en la página 421)
[Grupo predeterminado y asignatario](#) (en la página 426)
[Activación de la asignación automática](#) (en la página 427)
[Sustitución con la asignación automática](#) (en la página 428)
[Controles de asignación](#) (en la página 429)
[Registro de actividades](#) (en la página 432)
[Seguimiento de asignación automática](#) (en la página 432)
[Consultas almacenadas](#) (en la página 433)
[Cómo asigna tickets la función Asignación automática](#) (en la página 433)
[Cómo asigna tareas de workflow la función Asignación automática](#) (en la página 440)
[Asignaciones automáticas basadas en el elemento de configuración](#) (en la página 443)

Asignación automática

La *Asignación automática* de CA Service Desk Manager puede reducir en gran medida el tiempo necesario para gestionar tickets automatizando el proceso asignación de tickets a analistas. Esta automatización puede hacer que las tareas asociadas con equilibrar cargas de trabajo y coordinar programaciones de trabajo sean mucho más eficaces.

Puede configurar la asignación automática para que se asignen tickets según los siguientes factores:

- Qué grupo de analistas trabaja en qué tickets o tareas
- Cuándo se debe hacer el trabajo
- Qué ubicaciones prestan servicio a los clientes afectados
- La carga de trabajo y disponibilidad de cada analista
- El valor de un atributo de un elemento de configuración asociado con el ticket

Nota: La asignación automática basada en elementos de configuración (see page 443) le permite crear asignaciones específicas de grupo para tickets de Solicitud/Incidente/Problema solamente.

No tiene que implementar la asignación automática en su totalidad de una vez. Puede desarrollar una estrategia para introducirla gradualmente. Por ejemplo, puede empezar por habilitarla solamente para los tipos de ticket, grupos de analista o ubicaciones seleccionados.

Relaciones de asignación automática

El proceso de asignación automática puede implicar muchos elementos de CA Service Desk Manager. Las relaciones de elementos son las siguientes:

- Las áreas y categorías se relacionan con los grupos, las ubicaciones y los turnos.
- Los grupos se relacionan con las ubicaciones y los turnos.
- Las plantillas de CA Workflow se relacionan con los contactos.

Con objeto de facilitar la administración de la asignación automática, el mantenimiento de todas las relaciones se puede realizar desde cualquier elemento relacionado. Por ejemplo, al relacionar un grupo de analistas con una categoría de cambio puede mantener la asociación desde la página Detalles de la categoría de cambio o la página Detalles de grupo.

Métodos de asignación automática

Los siguientes métodos básicos permiten asignar tickets de forma automática:

Asignación automática basada en la ubicación

Crea asignaciones para todos los tipos de ticket con base en lo siguiente:

- Las áreas y categorías relacionadas con los grupos, las ubicaciones y los turnos
- Los grupos relacionados con las ubicaciones y los turnos
- Las plantillas de CA Workflow relacionadas con los contactos

Nota: La asignación automática basada en la ubicación se denomina simplemente asignación automática.

Asignación automática basada en el elemento de configuración

Crea asignaciones de grupo para los tipos de ticket de incidente, problema y solicitud con base en lo siguiente:

- Las áreas que están relacionadas con tickets asociados a elementos de configuración
- Los atributos del elemento de configuración utilizados para registrar información de contacto o grupo

La asignación automática basada en la ubicación y la asignación automática basada en el elemento de configuración son opciones exclusivas porque se puede seleccionar solamente un algoritmo para usarse en determinada área de solicitud/incidente/problema. Los métodos de asignación automática basados en la ubicación y en el elemento de configuración sirven para asignar tickets cuando estos se crean. Sin embargo, la asignación automática basada en el elemento de configuración es distinta porque también vuelve a evaluar las asignaciones para un ticket siempre que se cambia el área o el elemento de configuración de un ticket de solicitud/incidente/problema. Si se especifica la asignación automática basada en el elemento de configuración pero no se genera correctamente una asignación de grupo para un ticket, se consulta la opción `Area_Defaults` a fin de determinar si deben utilizarse los valores predeterminados de Grupo y Asignatario para asignar el ticket.

Cómo empezar a implementar la asignación automática

Siga estas directrices para empezar a implementar la asignación automática para los grupos de analistas y analistas seleccionados:

1. Identifique una o más áreas o categorías para las cuales quiere habilitar la asignación automática.
Nota: Para revisar las configuraciones de área y categoría de su sitio, examínelas en la interfaz Web de CA Service Desk Manager. Para obtener instrucciones, consulte la *ayuda en línea*.
2. De forma predeterminada, la asignación automática está deshabilitada. Actívela sólo para las áreas y categorías (see page 421) en las que desee utilizarla.
3. Cree relaciones entre un área o categoría identificada y los grupos de analistas (see page 422) que sean aptos para la asignación de tickets a través de esa área o categoría.
4. Marque a miembros individuales de los grupos de analistas (see page 423) como disponibles.

Áreas y categorías

Nota: Al configurar áreas y categorías, establezca la configuración de grupos y asignatarios predeterminados (see page 426).

Para configurar asignaciones automáticas de tickets de solicitud, incidente y problema, utilice los siguientes controles de la ficha Asignación automática de la página Detalles de área de solicitud/incidente/problema:

- Actualizar grupos
- Actualizar ubicaciones
- Actualizar turnos

Nota: La casilla de verificación para habilitar la asignación automática también se encuentra en la ficha Asignación automática de cada una de estas páginas. Aparece solamente mientras la página está en modo Edición.

Las siguientes páginas de la interfaz proporcionan los mismos controles para configurar la asignación automática de órdenes de cambio e incidencias:

- Detalles de categoría de cambio
- Detalles de categoría de incidencias

Grupos de analista

Para configurar la asignación automática debe, por lo menos, definir las relaciones entre grupos de analista y áreas o categorías. Los asignatarios se eligen de los grupos que cumplen *todos* los criterios de asignación automática especificados. Si no se han definido más restricciones, los tickets se asignan automáticamente al miembro del grupo con el menor número de tickets activos.

Si no se ha asociado ningún grupo al área o categoría, se asignan el grupo y el asignatario predeterminados. Si no se han definido estos valores predeterminados, se deja el ticket para la asignación manual.

Puede mantener las relaciones entre grupos y áreas o categorías en la página de detalles de área o categoría.

Alternativamente, puede mantener las mismas relaciones en la ficha Asignación automática de la página Detalles de grupo mediante los siguientes controles:

- Actualizar áreas de solicitud
- Actualizar categorías de cambio
- Actualizar categorías de incidencia
- Actualizar ubicaciones

Analistas

Los campos de la página Detalle de analista determinan si el analista es elegible para la asignación automática.

Los analistas son elegibles para la asignación automática solamente si se marcan como disponible.

La página Detalle de analista proporciona una casilla de verificación Disponible que habilita la asignación automática.

Una alternativa es permitir que los analistas controlen su disponibilidad para esta función. Puede controlar la disponibilidad de los analistas mediante consultas almacenadas.

Nota: La casilla de verificación Disponible no se considera durante asignación automática de tareas de workflow.

El campo Programación de trabajo permite la asignación automática de tickets a los analistas solamente durante su turno programado. Los analistas que no tienen ninguna programación de trabajo asignada, pero están marcados como disponibles son elegibles para la asignación automática en cualquier momento, siempre que no haya ninguna otra restricción que dé lugar a un estado inelegible.

Asignación automática por ubicación

Si el área de servicio es grande y consta de muchas ubicaciones que atienden a comunidades de clientes diferentes, puede utilizar la ubicación como un factor de configuración de la asignación automática como se indica a continuación:

- **Asignación de una ubicación a un área o categoría:** si asigna una ubicación a un área o a una categoría, los tickets de esa área o categoría sólo se asignarán automáticamente si se encuentra la ubicación correspondiente. Por ejemplo, un ticket de solicitud se asigna automáticamente si hay un analista disponible en las ubicaciones siguientes:

1. La ubicación del activo afectado
2. La ubicación del cliente afectado

Si el cliente o activo afectados no tienen especificada ninguna ubicación, la solicitud se asigna al asignatario y grupo predeterminados. Si no se han definido dichos valores predeterminados, se deja la solicitud para su asignación manual. Puede utilizar las páginas de detalles de área o categoría para mantener relaciones entre ubicaciones y áreas o categorías.

- **Asignación de una ubicación a un grupo:** si asocia una ubicación a un grupo, sólo los miembros de dicho grupo serán aptos para la asignación automática de los tickets que pertenecen a su ubicación. Puede utilizar páginas de detalles de grupo para mantener relaciones entre grupos y ubicaciones.

Para mantener las relaciones de las ubicaciones con áreas, categorías o grupos, utilice los controles siguientes de la ficha Asignación automática de la página Detalles de ubicación:

- Actualizar áreas de solicitud
- Actualizar categorías de cambio
- Actualizar categorías de incidencia
- Actualizar grupos

Ejemplos: utilización de ubicación en la configuración de asignación automática

Los siguientes son ejemplos de cómo puede utilizar ubicaciones en la configuración de asignación automática:

- **Asignar automáticamente tickets sólo a una ubicación especificada:** los tickets de otras ubicaciones reciben los asignatarios y grupos predeterminados o se reservan para la asignación manual. Por ejemplo, puede que haya muchos usuarios en la sede de la empresa y grupos más pequeños de usuarios en las oficinas regionales. Un grupo de analistas situado en la sede atiende a los usuarios locales, mientras los grupos móviles de analistas visitan las oficinas regionales. Puede configurar la asignación automática de tickets únicamente a los analistas de la sede y asignar manualmente los tickets a los analistas móviles.
- **Asignar automáticamente tickets por ubicación del activo o del usuario:** puede restringir la inclusión en la asignación automática a grupos de analistas de ubicaciones que coincidan con la ubicación del usuario afectado o con la ubicación del activo afectado. Por ejemplo, si la organización cuenta con muchas oficinas y los tickets de cada oficina sólo los gestionan los grupos ubicados en dicha oficina, Puede relacionar cada grupo a áreas o categorías apropiadas y a la ubicación apropiada. La lógica de la asignación automática seleccionará a los analistas adecuados sólo de los grupos que se encuentren en la ubicación correcta.

Asignación automática por turno

Se pueden aplicar ciertas restricciones a la asignación automática relacionando áreas o categorías con un turno. El turno determina el marco temporal dentro del cual los tickets están disponibles para la asignación automática. Los tickets abiertos fuera de las horas del turno se asignan al grupo y analista predeterminados o se dejan para la asignación manual.

Puede utilizar también turnos para controlar la elegibilidad del grupo y de analistas para la asignación:

- Si asigna una programación de trabajo a un grupo, los analistas de ese grupo son elegibles para la asignación automática sólo de los tickets abiertos durante su programación de trabajo.

Nota: El turno de un grupo se especifica en el campo Programación de trabajo de la página Detalles de grupo.

- Si asigna una programación de trabajo a un analista individual, el analista es elegible para la asignación automática sólo de los tickets abiertos durante esa programación de trabajo.

Nota: El turno de un analista se especifica en el campo Programación de trabajo de la página Detalles de grupo.

Durante la creación de tickets, la lógica de la asignación automática intenta identificar al analista con la menor cantidad de tickets activos del grupo que reúna los criterios de elegibilidad de asignación. Si no se identifica a un analista apropiado, el ticket se asigna al grupo predeterminado y asignatario. Si no se han definido estos valores predeterminados, se deja el ticket para la asignación manual.

Cuando se trata de tareas de workflow asociadas a órdenes de cambios o incidencias, la función de asignación automática pone en práctica una estrategia de selección más sencilla. Los asignatarios son seleccionados de grupos asociados a las plantillas de workflow. Estos asignatarios de tareas de workflow pueden pertenecer a cualquier tipo de contacto, excepto el grupo. Cuando alguna tarea cambia al estado Pendiente, la asignación automática selecciona al contacto con el menor número de tareas de workflow de órdenes de cambios o incidencias asignadas. A fin de evitar resultados inesperados, si la categoría de orden de cambio o de incidencia principal no tiene activada esta función, las tareas no se asignan de forma automática. Como las tareas de workflow pueden abarcar a personas ajenas a la organización de centro de servicio al usuario y confiar en ellas para que reflejen su disponibilidad con exactitud con el indicador Disponible podría resultar problemático.

Nota: La asignación automática de tareas de workflow no evalúa el indicador Disponible y no está disponible para las categorías configuradas para usar el procesamiento de CA Workflow.

Puede utilizar las páginas de detalles de área o categoría para relacionar un turno con un área o categoría, o puede utilizar los controles siguientes en la página Detalles de turno:

- Actualizar áreas de solicitud
- Actualizar categorías de cambio
- Actualizar categorías de incidencia

Ejemplos: utilización de turnos en la configuración de asignación automática

Los siguientes son ejemplos de cómo puede utilizar turnos en su configuración de asignación automática:

- **Asignar automáticamente tickets al turno activo:** si el servicio de asistencia funciona las 24 horas del día, puede que desee configurar la asignación automática de forma que los problemas de interrupción de la red se asignen al turno activo al abrir el ticket.
- **Permitir la asignación automática sólo durante un turno especificado:** puede que desee restringir aún más la asignación automática de los tickets en algunas áreas o categorías. Por ejemplo, si los analistas de aplicaciones de un sitio están de servicio solamente durante el turno de día, es posible que desee asignar automáticamente problemas de aplicación solamente durante el turno de día.

Grupo predeterminado y asignatario

Cuando la lógica de asignación automática que ha configurado no puede identificar un grupo apropiado o asignatario, el ticket se asigna al grupo y asignatario predeterminados. Puede especificar estos valores predeterminados en los campos Grupo y Asignatario de las siguientes páginas de interfaz Web:

- Detalles de área de solicitud/incidente/problema
- Detalles de categoría de cambio
- Detalles de incidencia

Si la asignación automática no puede identificar un grupo o asignatario apropiado y los valores predeterminados no se especifican, el ticket queda para la asignación manual.

Activación de la asignación automática

Las opciones y los controles permiten configurar la asignación automática. Puede controlar si el procesamiento de asignación automática ocurre del siguiente modo:

- Para solicitudes, incidentes y problemas asignados a esa área, utilice la ficha Asignación automática activada de la página Detalles de área de solicitud/incidente/problema.
- Para órdenes de cambio, incidencias y tareas de workflow, seleccione la ficha Asignación automática y la casilla de verificación Asignación automática activada de las páginas Detalles de categoría de cambio, Detalles de categoría de incidencia y Detalles de plantilla de CA Workflow.

Nota: Haga clic en Editar para que aparezca la casilla de verificación Asignación automática activada.

Ejemplo: habilitación de la asignación automática para un área de solicitud/incidente/problema

En este ejemplo se demuestra cómo habilitar la asignación automática para un área de solicitud/incidente/problema.

1. En la ficha Administración, vaya a Service Desk, Solicitudes/Incidentes/Problemas, Áreas.
Aparece la página Lista de áreas de solicitud/incidente/problema.
2. Haga clic en el área en la que quiere configurar la asignación automática.
Aparece la página Detalles de áreas de solicitud/incidente/problema.
3. Haga clic en Editar.
Aparece la página Actualizar áreas de solicitud/incidente/problema.

4. Seleccione la ficha Asignación automática y complete los campos a continuación de la siguiente forma:

Modo de asignación automática

Especifica cómo se produce la asignación automática. Puede utilizar la opción basada en el elemento de configuración para basar la asignación automática en el valor de atributo asignable de CI.

- **Desactivado:** Basa la asignación automática en la opción Valores predeterminados de área cuándo está instalada.
- **Basado en elemento de configuración:** Basa la asignación automática en el valor Atributo de elemento de configuración asignable.
- **Basado en ubicación:** Basa la asignación automática en el valor Ubicación.

Atributo de elemento de configuración asignable

Especifica el atributo de elemento de configuración que se va a utilizar para la asignación de grupo. Puede introducir un valor directamente o hacer clic en la lupa para buscar un atributo.

5. Haga clic en Guardar.

Las áreas de solicitud/incidente/problema permiten usar valores predeterminados introducidos automáticamente en los tickets de solicitudes, incidentes o problemas asignados a un área en particular.

Sustitución con la asignación automática

Puede usar la opción de sustitución con asignación automática (autoasg_override) del Gestor de opciones para determinar si la asignación automática debe sustituir al analista o grupo que se haya definido durante la creación de los tickets.

Es posible que otras funciones de CA Service Desk Manager hayan definido el asignatario o el grupo antes de que la asignación automática tome el control. Para personalizar su sistema, defina esta opción con uno de los siguientes valores:

0

Respeta al asignatario o al grupo existentes. No se realizará el procesamiento de asignación automática si se ha definido el grupo y/o asignatario durante la creación del ticket.

1

Ignora al asignatario o al grupo existentes. El procesamiento de asignación automática continuará e intentará encontrar un asignatario y/o grupo.

Se puede definir el asignatario y/o grupo de varias maneras:

- Manualmente por el analista
- Mediante las opciones Valores predeterminados de área y Definición de asignatario
- Mediante plantillas de solicitud
- Integración de CA NSM

Nota: La desinstalación de la opción de sustitución con la asignación automática hace que funcione en su modo predeterminado, es decir, 0.

Controles de asignación

Las opciones y los controles permiten configurar la asignación automática. Existen otras funciones de CA Service Desk Manager que pueden afectar a los campos de asignatario o de grupo (o a ambos) de los tickets antes de que se produzca el procesamiento de la asignación automática. Recomendamos que revise los controles de asignación antes de implementar la asignación automática.

Asignación manual

El analista puede seleccionar manualmente al asignatario y/o grupo mientras crea un ticket.

Opción Assignee_set

De forma predeterminada, CA Service Desk Manager establecerá automáticamente el usuario conectado como asignatario de la solicitud, siempre que se trate de un analista. La opción Assignee_set del gestor de opciones permite controlar este comportamiento. Normalmente, esta opción se instala de forma predeterminada.

Opción Iss_assignee_set

La opción Iss_assignee_set define automáticamente al usuario conectado como asignatario de la incidencia, siempre que se trate de un analista. Es similar a Assignee_set, pero para incidencias en lugar de solicitudes.

Area_Defaults

Esta opción determina lo que sucede cuando se especifica el área de solicitud en la página de detalles de alguna solicitud. Esta opción permite establecer el asignatario y el grupo cada vez que cambia el área de solicitud. Se usan el asignatario y el grupo predeterminados del área de solicitud. Este procesamiento se efectúa antes que el procesamiento de asignación automática.

Esta opción se instala de forma predeterminada.

Nota: La opción Category_Defaults proporciona una funcionalidad similar para las órdenes de cambio. La opción Iss_Category_Defaults proporciona una funcionalidad similar para las incidencias.

Opciones de obligatoriedad de asignatario y grupo

Varias opciones están disponibles en el Gestor de opciones para controlar la creación de tickets no asignados. que tienen un ámbito global Afectan a la creación de todos los tipos de tickets indicados, independientemente de que se haya activado o no la asignación automática. Si no se cumple la condición señalada, no se permite guardar el ticket nuevo o actualizado.

Nota: Las opciones correspondientes para los incidentes y los problemas sólo están disponibles cuando el sistema está configurado para usar la metodología ITIL.

Las opciones siguientes controlan la creación de tickets sin un asignatario especificado:

require_change_assignee

Aplicación: gestor de órdenes de cambios

Descripción: hace que el campo Asignatario de un ticket de orden de cambio sea necesario

require_issue_assignee

Aplicación: gestor de incidencias

Descripción: hace que el campo Asignatario de un ticket de incidencia sea necesario

require_incident_assignee

Aplicación: gestor de solicitudes

Descripción: hace que el campo Asignatario de un ticket de incidente sea necesario

require_problem_assignee

Aplicación: gestor de solicitudes

Descripción: hace que el campo Asignatario de un ticket de problema sea necesario

require_request_assignee

Aplicación: gestor de solicitudes

Descripción: hace que el campo Asignatario de un ticket de solicitud sea necesario

Las opciones siguientes controlan la creación de tickets sin un grupo especificado:

require_change_group

Aplicación: gestor de órdenes de cambios

Descripción: hace que el campo Grupo de un ticket de orden de cambio sea necesario

require_issue_group

Aplicación: gestor de incidencias

Descripción: hace que el campo Grupo de un ticket de incidencia sea necesario

require_incident_group

Aplicación: gestor de solicitudes

Descripción: hace que el campo Grupo de un ticket de incidente sea necesario

require_request_group

Aplicación: gestor de solicitudes

Descripción: hace que el campo Grupo de un ticket de solicitud sea necesario

require_problem_group

Aplicación: gestor de solicitudes

Descripción: hace que el campo Grupo de un ticket de problema sea necesario

Plantillas

Las plantillas se pueden utilizar para definir valores en la solicitudes, las órdenes de cambio o las incidencias nuevas. Los campos de asignatario y grupo son algunos de los que se ven afectados por las plantillas.

Interfaz de CA Network and Systems Management

Cuando se han integrado CA NSM y CA Service Desk Manager, y se crean peticiones desde eventos de CA NSM, el parámetro `user_parms` de las definiciones de reglas de escritura se traslada al API de texto. El proceso de escritura de CA Service Desk Manager (tngwriter) define sus propios parámetros de reemplazo para cambiar el texto antes de enviarlo a Text API. La palabra clave `LOG_AGENT` se agrega al final de la entrada para establecer el `log_agent` para la petición.

Nota: Necesita actualizar el archivo `Text_API.cfg` para todos los campos adicionales que se trasladan desde los sistemas de gestión de alertas de CA NSM a CA Service Desk Manager. Este archivo se utiliza para integraciones con servicios Web, correo electrónico y AHD.DLL.

Más información:

[Palabras clave](#) (en la página 476)

Registro de actividades

La función de asignación automática registra la información en forma de eventos en los registros de actividades de los tickets. El éxito o el fracaso de la asignación automática queda registrado, así como cualquier anomalía que pueda haber ocurrido durante el procesamiento.

Seguimiento de asignación automática

En implementaciones de asignación automática complejas, es posible que esta función no adopte las decisiones esperadas. El seguimiento, si está activado, ayuda a entender el flujo del procesamiento. Por norma general, el seguimiento se encuentra desactivado. Ahora bien, si se activa, se escriben numerosos mensajes en los archivos `stdlog` de `$NX_ROOT\log` en los que se describen las diversas decisiones adoptadas por la asignación automática.

Por este motivo, es necesario tener cuidado al activarla en instalaciones con un gran volumen de actividad, ya que el número de mensajes generados puede hacer crecer tanto los archivos de registro que se llegue a solapar el contenido. En los sistemas de gran actividad, es posible que se vea afectado el rendimiento. El seguimiento se controla con la utilidad `pdm_logstat`. En los parámetros empleados con esta utilidad se distingue entre mayúsculas y minúsculas. Por ello, cerciórese de escribirlos tal como se muestra.

Para activar el seguimiento, utilice el siguiente comando en el servidor:

```
pdm_logstat -f auto.pm milestone
```


Para desactivar el seguimiento, utilice el siguiente comando en el servidor:

```
pdm_logstat -f auto.pm
```

Consultas almacenadas

Se suministran dos consultas almacenadas para controlar la disponibilidad de los analistas. Los gestores de CA Service Desk Manager pueden agregar lo siguiente a su panel de resultados:

- **Analistas disponibles:** analistas que son marcados como disponible para la asignación automática
- **Analistas no disponibles:** analistas que son marcados como no disponible para la asignación automática

Cómo asigna tickets la función Asignación automática

La asignación automática asigna tickets del siguiente modo:

1. La operación de guardado inicial de un ticket nuevo invoca la asignación automática.

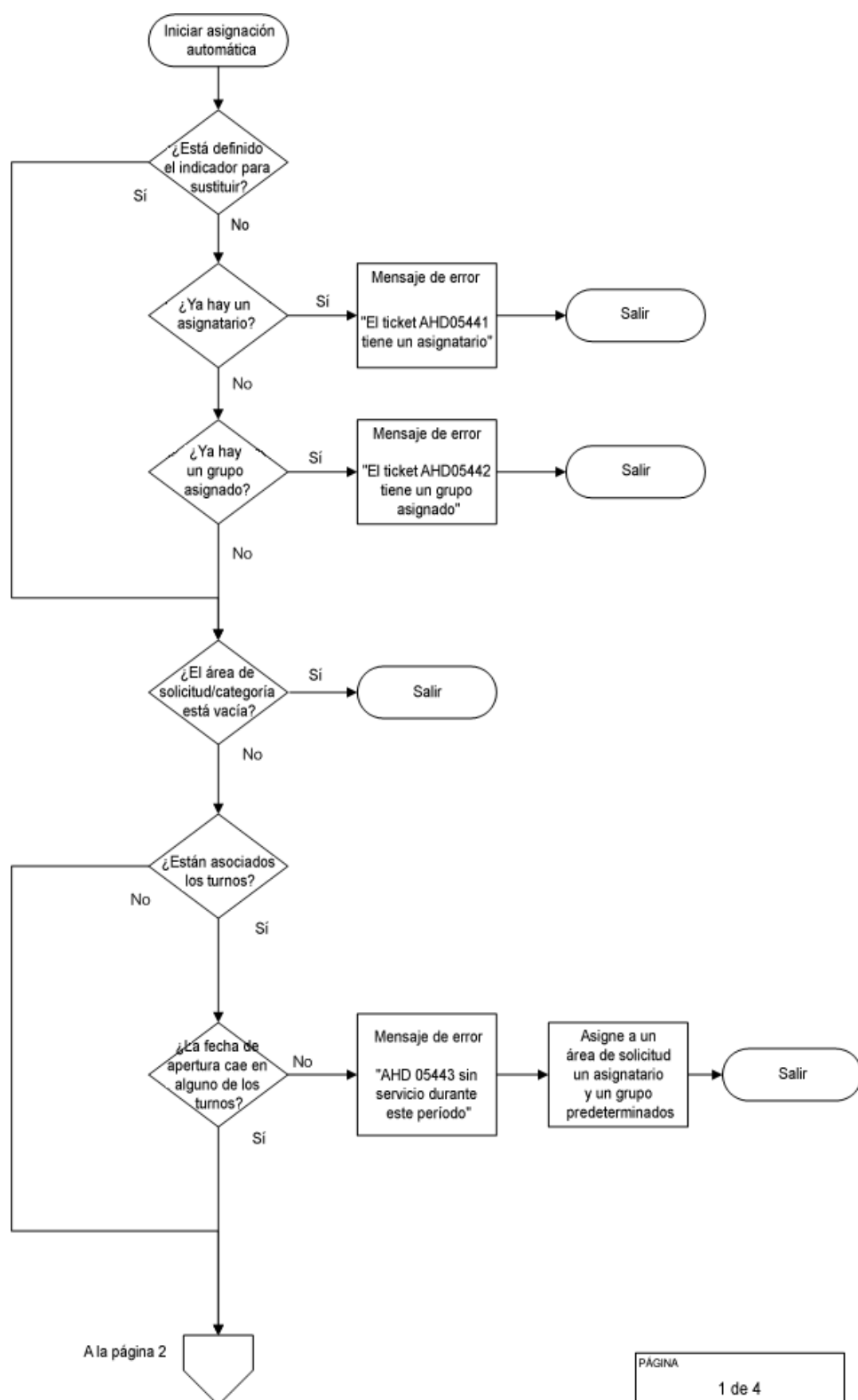
Si no se configura un área o categoría para la asignación automática, el procesamiento se detiene.
2. La asignación automática determina si se instala Autoasg_override.

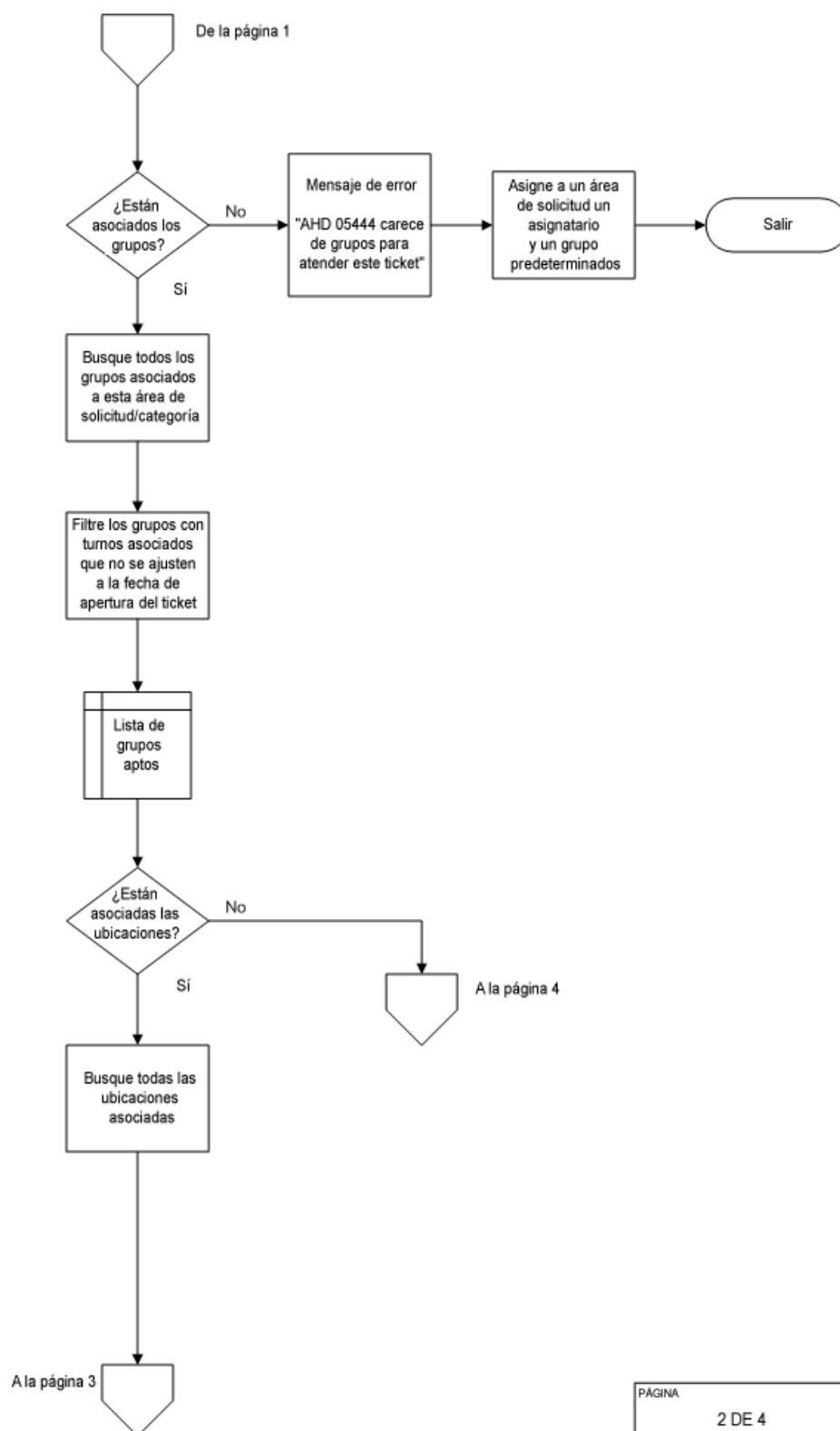
Si no lo está y el ticket en cuestión dispone de un asignatario o grupo, se detiene el procesamiento.
3. Si se relacionan turnos con el ticket, la fecha abierta se evalúa para determinar si un turno incluye el ticket.

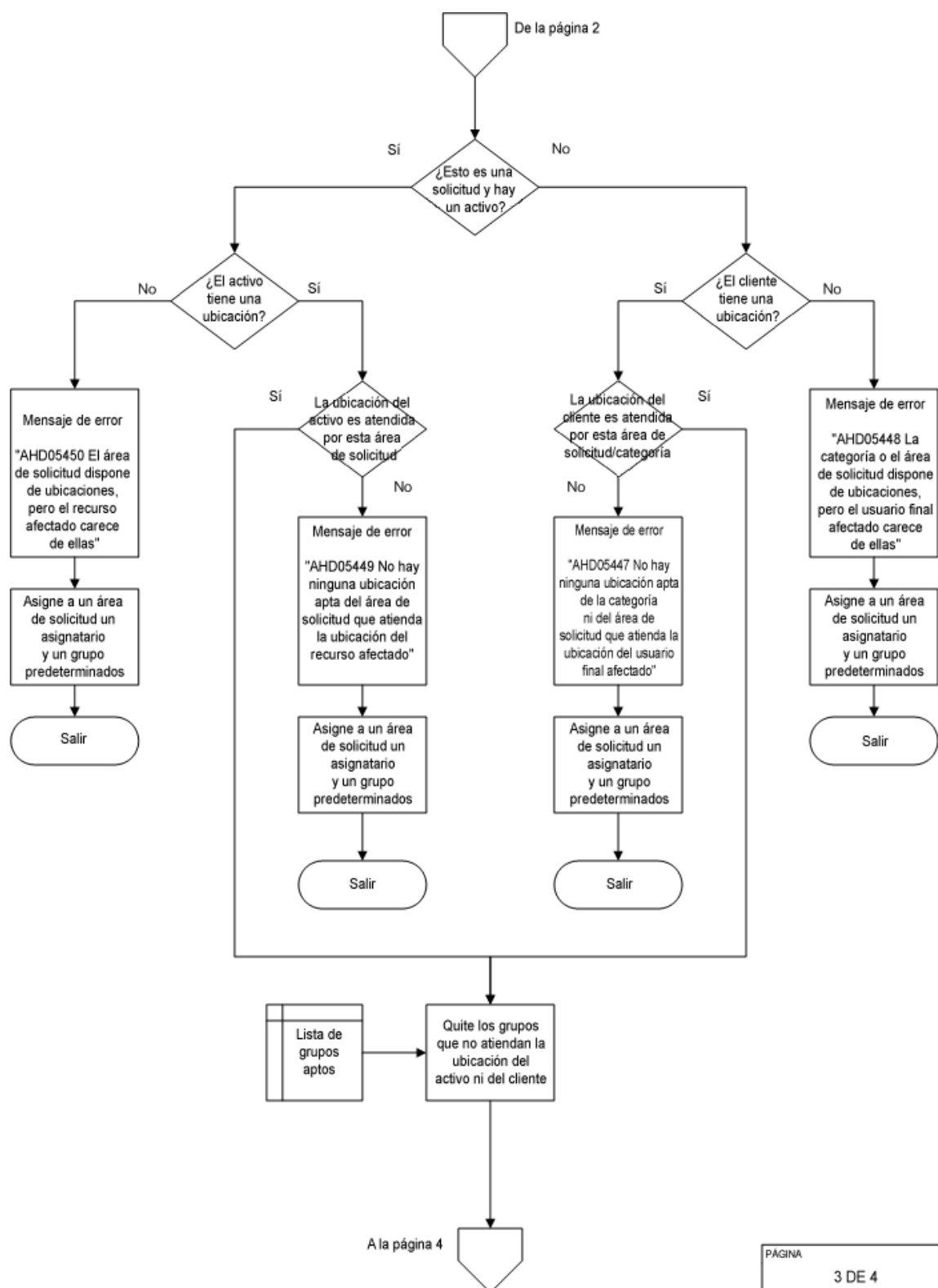
Si un turno no incluye el ticket, el procesamiento se detiene y la asignación automática intenta asignar el grupo y asignatario predeterminados.
4. La asignación automática determina si algún grupo se relaciona con el ticket.

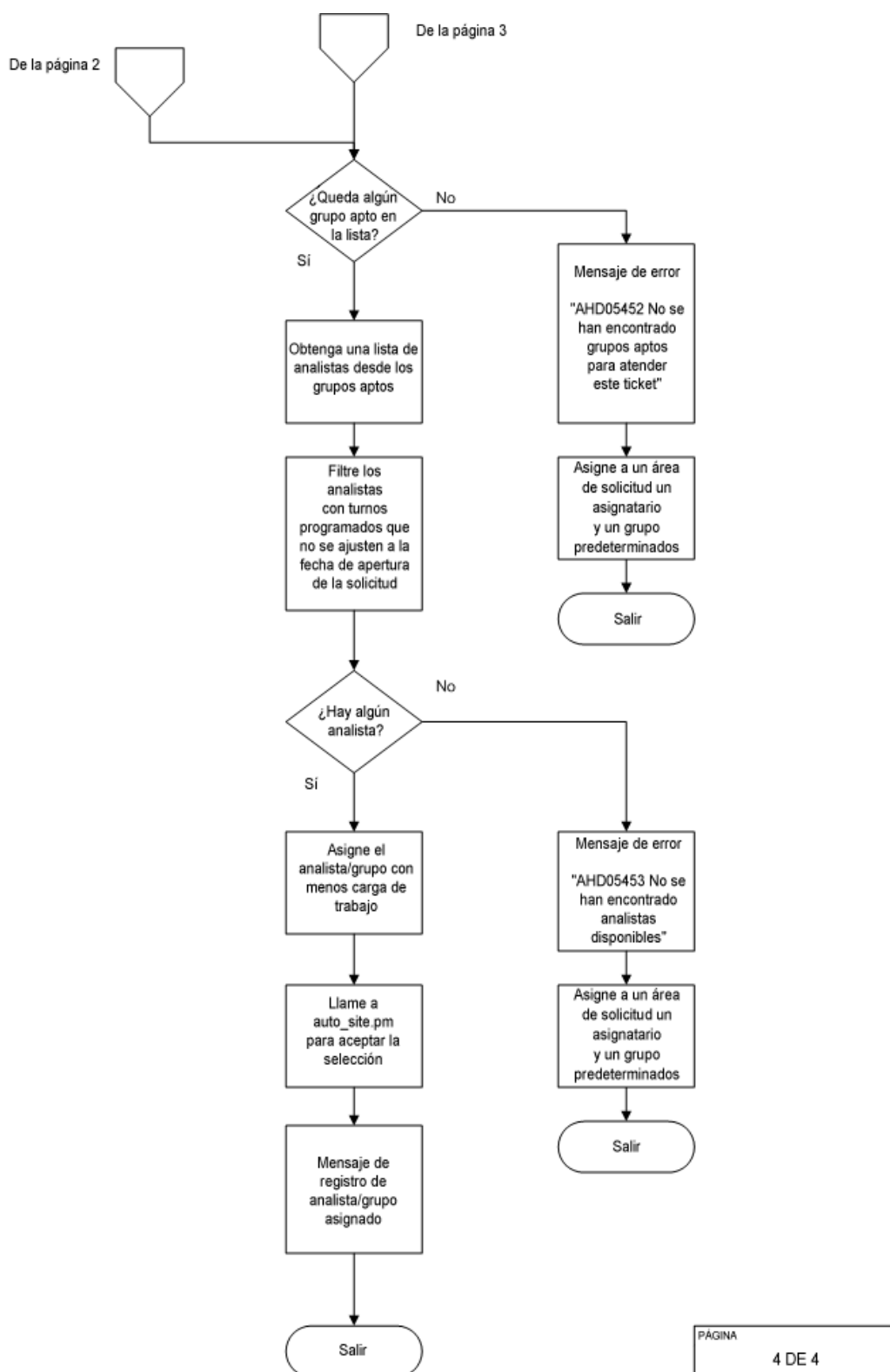
En caso de que no haya coincidencia, se detiene el procesamiento y la asignación automática intenta asignar el grupo y el asignatario predeterminados.
5. La asignación automática filtra algunos grupos con un turno asociado, donde la fecha abierta está fuera del marco de tiempo del turno. El filtro deja pasar los grupos que carezcan de turno.

6. Lo siguiente ocurre en ubicaciones que se relacionan con el ticket:
 - Si este ticket es una solicitud y tiene un elemento de configuración
La ubicación del elemento de configuración se compara con las ubicaciones relacionadas con el área de solicitud. En caso de que no haya coincidencia, se detiene el procesamiento y la asignación automática intenta asignar el grupo y el asignatario predeterminados. De lo contrario, se compara la ubicación del cliente con las ubicaciones relacionadas con el área o la categoría. En caso de que no haya coincidencia, se detiene el procesamiento y la asignación automática intenta asignar el grupo y el asignatario predeterminados.
 - Si se han asociado ubicaciones con el área de solicitud o la categoría
Si se han asociado ubicaciones al área de solicitud y al elemento de configuración (durante el procesamiento de asignación automática de solicitudes) o el cliente carece de ubicación, la asignación automática detiene el procesamiento.
7. La asignación automática descarta los grupos aptos con ubicaciones relacionadas que no coincidan con la ubicación del elemento de configuración (sólo en el caso de las solicitudes) o del cliente. Si no quedan grupos, se detiene el procesamiento y la asignación automática intenta asignar el grupo y el asignatario predeterminados.
8. La asignación automática crea una lista de analistas de cada uno de los grupos aptos restantes.
9. Se descartan los analistas que no estén disponibles.
10. Entonces se comprueban las programaciones de trabajo de los demás analistas. Si la fecha de apertura no se encuentra dentro de la programación de trabajo del analista, éste se descarta.
11. Si no quedan analistas, se detiene el procesamiento y la asignación automática intenta asignar el grupo y el asignatario predeterminados.
12. Los analistas restantes se clasifican según el número de tickets activos que tengan asignados.
13. Se asigna el ticket al analista (y grupo asociado) que cuente con el menor número de tickets activos. En caso de empate, se elige el primer analista del grupo.





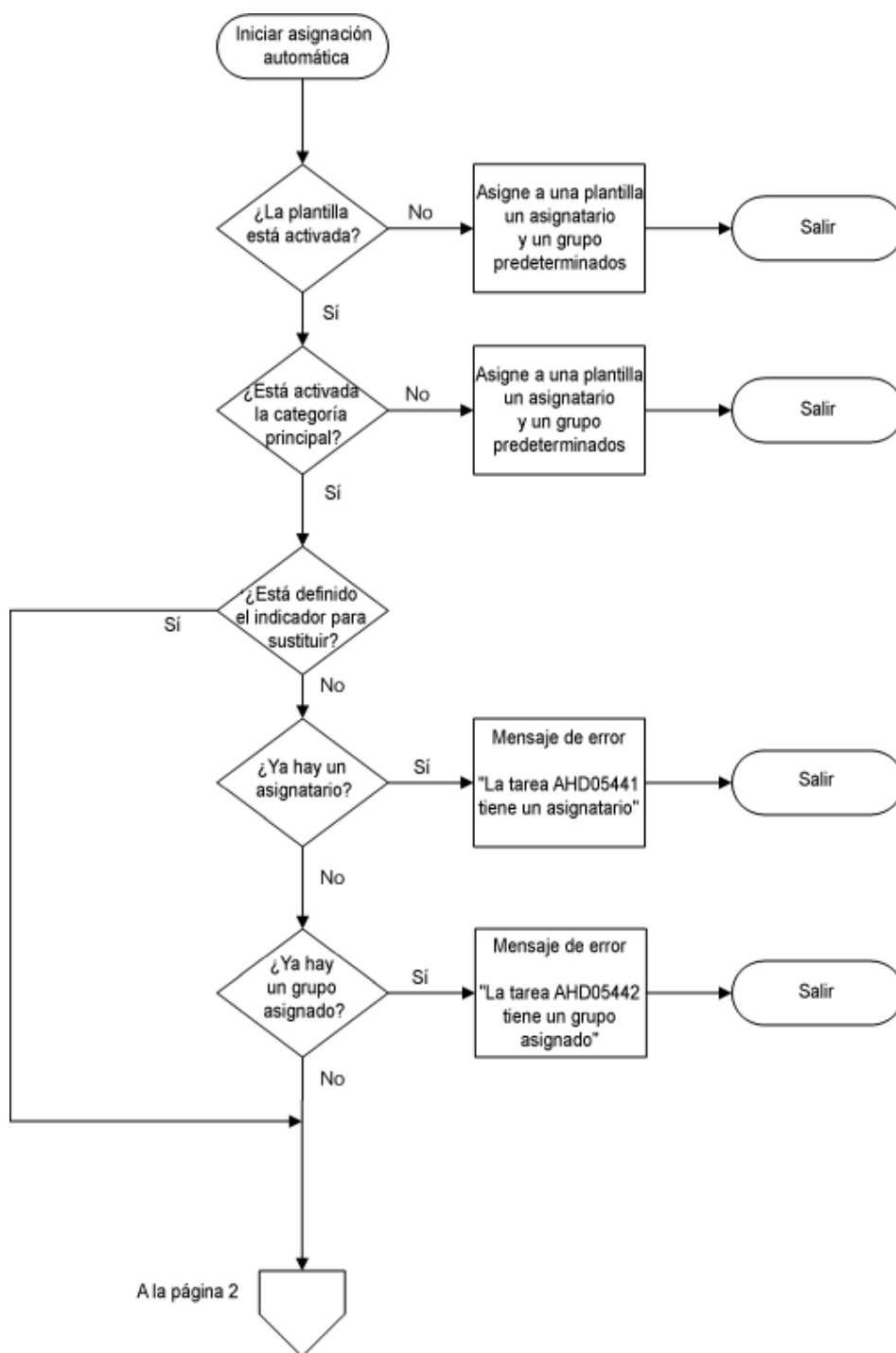


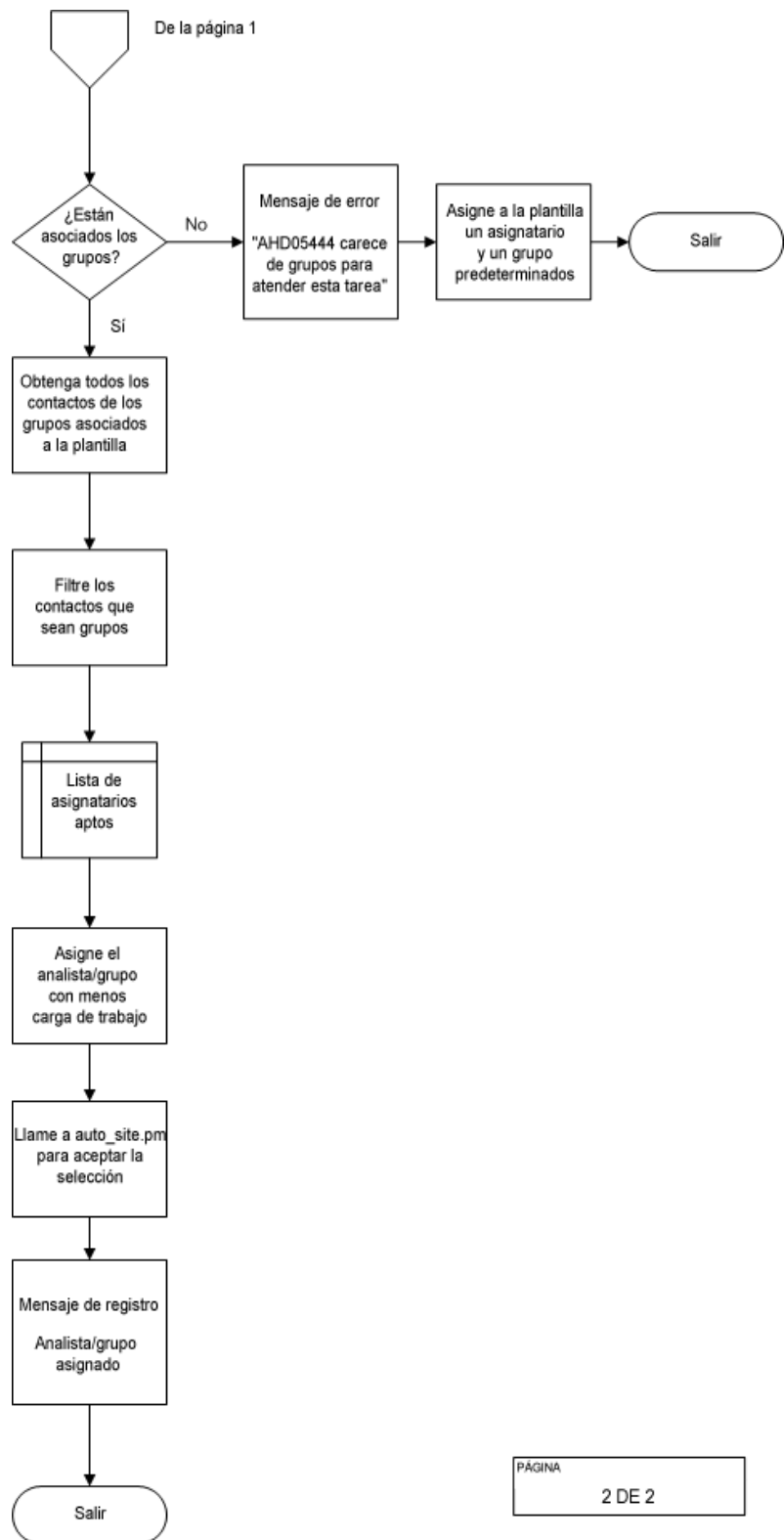


Cómo asgina tareas de workflow la función Asignación automática

La función de asignación automática utiliza la lógica de procesamiento para asignar tareas de workflow de la siguiente manera:

1. La función de asignación automática se invoca cuando el estado de las tareas de workflow cambia a pendiente. Si la plantilla de workflow a partir de la cual se creó la tarea de workflow pertinente no está habilitada para la asignación automática, se detiene el procesamiento. Si la categoría de órdenes de cambios o incidencias principal no tiene habilitada esta función, se detiene el procesamiento.
2. La función de asignación automática comprueba si está instalada la opción `Autoasg_override`. Si no lo está y la tarea en cuestión dispone de un asignatario o grupo, se detiene el procesamiento.
3. Se comprueba la plantilla de workflow a partir de la cual se creó la tarea de workflow pertinente para verificar si tiene asociado algún contacto. Si no existe ningún contacto, se detiene el procesamiento.
4. La función de asignación automática crea una lista de todos los contactos que sean miembros de los grupos asociados actualmente a la plantilla de workflow a partir de la cual se creó la tarea de workflow. Se descartan todos los contactos de dicha lista que sean grupos.
5. Los contactos restantes se clasifican según el número de tareas de órdenes de cambios o de incidencias activas que tengan asignadas.
6. Entonces se asigna la tarea al contacto y grupo asociado que cuenten con un menor número de tareas activas.





Asignaciones automáticas basadas en el elemento de configuración

Las asignaciones automáticas basadas en el elemento de configuración permiten crear asignaciones específicas de grupo que se aplican a escenarios específicos. Puede especificar que para los tickets de petición/incidente/problema abiertos para un área determinada, el valor de un atributo del elemento de configuración asociado con el ticket controle su asignación.

Las asignaciones automáticas basadas en la ubicación y en el elemento de configuración son opciones exclusivas porque es posible seleccionar solamente un algoritmo para usar en un área de solicitud/incidente/problema. Los modos de asignación automática tanto basada en elementos de configuración como basada en ubicación sirven para asignar tickets cuando se crean. Sin embargo, la asignación automática basada en elementos de configuración es distinta porque también vuelve a asignar tickets cuando el área de petición/incidente/problema de un ticket o elemento de configuración se cambia.

Ejemplo: el área de petición/incidente/problema asigna tickets a un grupo

Cuando configura el área de red (para peticiones/incidentes/problemas) para ejecutar las asignaciones automáticas basadas en elementos de configuración que utilizan el atributo `network_contact_uuid` (Operaciones de red) como el valor de Atributo de elemento de configuración asignable, los tickets que se abren para el área de red se asignan automáticamente al grupo especificado en el campo Operaciones de red del CI asociado con el ticket. Si no se asocia ningún CI con el ticket, o si el valor del campo Operaciones de red del CI está vacío o no especifica un grupo, no se produce la asignación. En tales casos, el sistema actúa de acuerdo con la opción Gestor de opciones, Valores predeterminados del área, y asigna el ticket que utiliza los campos Grupo y Asignatario de la categoría.

Cómo funciona la asignación automática basada en el elemento de configuración

Los tickets de solicitud/incidente/problema deben especificar lo siguiente para que se produzca la asignación automática basada en el elemento de configuración:

- Un elemento de configuración y un área.
- El área debe tener la opción Asignación automática establecida en Basada en el elemento de configuración.

Cuando un analista crea y asigna un ticket a esta área, o cambia el área de un ticket existente, CA Service Desk Manager examina el campo Atributo de elemento de configuración asignable del área. CA Service Desk Manager utiliza el valor del Atributo de elemento de configuración asignable como el nombre de un atributo y, a continuación, intenta encontrar un atributo con nombre idéntico en el elemento de configuración asociado con el ticket. Si el atributo del elemento de configuración incluye un grupo, el ticket se asigna a dicho grupo.

El siguiente diagrama describe más detalladamente el proceso para la asignación automática basada en el elemento de configuración:

1. CA Service Desk Manager busca lo siguiente:
 - a. ¿Está establecida la opción `autoasg_override`?
 - b. ¿Especifica un ticket el área con su asignación automática `auto_assign_mode=2`?
 - c. ¿Especifica la categoría un atributo de elemento de configuración asignable?
 - d. ¿Especifica el ticket un elemento de configuración?
 - e. ¿Tiene el elemento de configuración un valor de atributo de elemento de configuración asignable?
 - f. ¿Especifica el valor un grupo en el atributo de elemento de configuración?
 - g. ¿Es el asignatario del ticket un miembro del grupo de tickets?
2. Cuando las respuestas son positivas para todas las preguntas del paso anterior, CA Service Desk Manager establece el atributo de grupo del ticket en el atributo de grupo del elemento de configuración y registra la asignación en el registro de actividades.

Nota: El diagrama muestra cómo la asignación automática basada en el elemento de configuración usa la variable `NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS` para determinar si se habilita la opción del área. `NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS` es una variable en el archivo `NX.env`, que se localiza en el directorio `$NX_ROOT\`.
3. CA Service Desk Manager asigna el ticket al grupo.

Más información:

[Sustitución con la asignación automática](#) (en la página 428)

Habilitación de asignaciones automáticas basadas en el elemento de configuración

Las asignaciones automáticas basadas en el elemento de configuración permiten crear asignaciones específicas de grupo que se aplican a escenarios específicos. Puede especificar que para los tickets de solicitud/incidente/problema abiertos para un área determinada, el valor de un atributo del elemento de configuración asociado con el ticket controle su asignación. La asignación automática basada en el elemento de configuración vuelve a asignar tickets cada vez que cambia el área de solicitud/incidente/problema de un ticket o elemento de configuración.

Nota: La opción `autoasg_override` del gestor de opciones controla las circunstancias bajo las que se produce una asignación automática. Al establecer esta opción en 1, CA Service Desk Manager omite cualquier asignatario existente y grupo de configuración, y asigna automáticamente tickets en todos los casos. Si desea que CA Service Desk Manager sólo asigne tickets automáticamente si aún no se han asignado, defina el valor de la opción en 0.

Procedimiento para habilitar la asignación automática basada en el elemento de configuración

1. En la ficha Administración, vaya a Service Desk, Solicitudes/Incidentes/Problemas, Áreas.
Aparecerá la lista de áreas de solicitud/incidente/problema.
2. Seleccione el área que desea editar.
Aparecerá la página Detalles de área.
3. Haga clic en Editar.
Aparecerá la página Actualizar área.
4. Seleccione la ficha Asignación automática y complete los campos de la siguiente forma:

Modo de asignación automática

Especifica cómo se produce la asignación automática. Puede utilizar la opción basada en el elemento de configuración para basar la asignación automática en el valor de atributo asignable de CI.

Atributo de elemento de configuración asignable

Especifica el atributo de elemento de configuración que se va a utilizar para la asignación de grupo. Puede introducir un valor directamente o hacer clic en la lupa para buscar un atributo.

Haga clic en Guardar.

Se activará la asignación automática. CA Service Desk Manager realiza asignaciones automáticas basadas en el elemento de configuración

mediante el atributo especificado en el campo Atributo de elemento de configuración asignable.

Capítulo 11: Gestión de su base de datos

Esta sección contiene los siguientes temas:

[Utilidades de la gestión de base de datos](#) (en la página 447)
[Selección y configuración de la base de datos](#) (en la página 447)
[Cargador de bases de datos](#) (en la página 448)
[Copia de seguridad de la base de datos](#) (en la página 451)
[Restauración de la base de datos](#) (en la página 451)
[Reemplazo de la tabla de base de datos](#) (en la página 452)
[Extracción de datos](#) (en la página 452)
[Anulación de referencias a datos](#) (en la página 454)
[Modo dbadmin](#) (en la página 457)
[Reglas de archivado y borrado definitivo](#) (en la página 458)

Utilidades de la gestión de base de datos

Puede ejecutar utilidades para gestionar su base de datos mientras se cierra CA Service Desk Manager. Si ejecuta las utilidades de gestión de las bases de datos y usa una base de datos que no sea el repositorio predeterminado de CA Service Desk Manager, es preciso definir las variables de entorno de la base de datos.

Nota: Para obtener información sobre la definición de variables del entorno, consulte la documentación de la base de datos que está utilizando.

Selección y configuración de la base de datos

Puede seleccionar la base de datos y configurarla para que CA Service Desk Manager la utilice.

Para seleccionar y configurar una base de datos

1. Seleccione la base de datos de la lista desplegable Tipo de base de datos y haga clic en Siguiente.

Aparecerá la página de configuración de la base de datos seleccionada.

2. Escriba la información de la base de datos en la página de configuración de la base de datos y haga clic en Siguiente.

Ha finalizado la configuración de la base de datos.

Nota: Utilice el botón Ayuda de esta página para obtener información de configuración sobre los campos de la base de datos seleccionada.

En las páginas de configuración, aparecen los botones siguientes.

Ayuda

Para acceder a la Ayuda de la página actual.

Cancelar

Para cancelar las opciones de configuración que ha realizado hasta ahora.

Atrás

Para ir a la página anterior sin guardar los cambios que haya realizado hasta ahora en la página actual.

Siguiente

Para acceder a la página siguiente después de guardar todos los cambios realizados en la página actual.

Cargador de bases de datos

La utilidad del cargador de bases de datos, `pdm_userload`, agrega, actualiza y suprime registros de base de datos de CA Service Desk Manager. Es preciso crear un archivo de entrada ASCII con formato para la utilidad `pdm_userload` y seleccionar las tablas para cargar así como los campos opcionales por agregar.

Importante: la utilidad `pdm_userload` accede a la base de datos de CA Service Desk Manager y no mantiene ninguna interacción directa con procesos de software de la aplicación. Los elementos de inventario agregados a las bases de datos con `pdm_userload` no actualizan las listas de selección ni de asistente hasta que se haya detenido y vuelto a iniciar la aplicación.

Aunque es posible ejecutar la utilidad `pdm_userload` mientras la aplicación sigue activa, el rendimiento del sistema se ve afectado. Para lograr un resultado óptimo, asegúrese de que el servidor de CA Service Desk Manager se esté ejecutando pero que ningún usuario esté utilizando la interfaz de cliente antes de ejecutar `pdm_userload`.

Nota: Si necesita agregar registros con campos con referencia cruzada, use la utilidad `pdm_deref`.

Más información:

[Anulación de referencias a datos](#) (en la página 454)

Cómo crear y utilizar un archivo de entrada

Puede utilizar un archivo de entrada y la utilidad `pdm_userload` para rellenar tablas de base de datos.

El formato del archivo de entrada es el siguiente:

- Valores de campo circundante con comillas dobles ("valor") y valores separados por un coma y un espacio ("valor1", "valor2").
- anteponga una barra inversa (\) a las comillas dobles para incrustarlas en cadenas de texto. Si desea definir un campo de fecha u hora según la fecha y la hora actuales, emplee `@NOW@` como valor de entrada.
- Rodee cada registro con llaves separadas por espacios, de la siguiente manera:

({ valores de los campos de los registros })

- Si se delimitan del modo adecuado, los registros de entrada pueden ocupar varias líneas del archivo de entrada siempre que cada uno de los campos permanezca en una sola línea. En el caso de los campos de varias líneas, como los de comentarios, los valores pueden incluir el carácter de salto de línea (\n) para que el texto que va a continuación pase a la línea siguiente cuando se muestre el campo de la base de datos.
- Los caracteres de nueva línea explícitos sólo son necesarios en el caso de formatos especiales. El texto corrido normal se muestra sin más con los saltos de línea adecuados, como se muestra en este ejemplo:

"El estado del registro es \"COMPLETE\""

Para crear un archivo de entrada para la utilidad `pdm_userload`, realice este procedimiento:

1. Determine la tabla que desee cargar y los campos de la tabla que desee rellenar.

Es necesario rellenar uno de los campos clave Nombre o Símbolo en todos los registros que se carguen.

2. Realice una copia del archivo *nombreakarchivo.dat* que corresponda a la tabla que pretenda cargar.
3. Edite la copia del archivo *nombreakarchivo.dat* recién creada del modo siguiente:

- a. Agregue una entrada por cada uno de los registros que vaya a cargar.

- b. Debajo de la línea TABLE (vea el ejemplo siguiente), elimine los campos que no desee rellenar.

```
TABLE nombre_tabla  
nombrecampo1 nombrecampo4. . . nombrecampoN
```

4. Guarde el archivo y salga del editor.
5. Ejecute la utilidad pdm_userload y especifique el archivo, como se muestra en el ejemplo siguiente. En este ejemplo, el nombre del archivo de entrada es myData.dat:

```
pdm_userload -f myData.dat
```

La tabla de base de datos se rellena.

Más información:

[pdm_userload: adición, actualización y eliminación de registros de las bases de datos](#) (en la página 1048)

Anulación y restauración de restricciones

Algunas de las tablas de MDB que comienzan por ca_ (como ca_contact_) cuentan con restricciones referenciales que pueden causar un impacto negativo en la carga masiva de datos mediante las herramientas pdm_load, pdm_userload y pdm_restore. En caso de que haga falta llevar a cabo la carga masiva de dichas tablas, quizá sea necesario anular las restricciones referenciales antes.

Se proporcionan dos secuencias de comandos SQL para cada tipo de DBMS para anular y restaurar restricciones. Antes de llevar a cabo la carga masiva de datos que afectan a tablas ca_*, ejecute la versión de anulación de la secuencia de comandos. Una vez finalizada la carga de datos, ejecute la versión de adición de la secuencia de comandos.

En el servidor SQL, los scripts están ubicados en *directorio de instalación/samples/views/SQLServer*. Para anular las restricciones ejecute el siguiente comando:

```
osql -E -e < SQLDropConstraints.sql'
```

Para volver a agregar restricciones, ejecute el siguiente comando:

```
osql -E -e < SQLAddConstraints.sql'
```

En Oracle, las secuencias de comandos están ubicadas en *directorio de instalación\samples\views\Oracle*.

Para anular las restricciones ejecute el siguiente comando:

```
sqlplus mdbadmin/ <contraseña> < OracleDropConstraints.sql
```

Para volver a agregar restricciones, ejecute el siguiente comando:

```
sqlplus mdbadmin/ <contraseña> < OracleAddConstraints.sql
```

Copia de seguridad de la base de datos

Se pueden realizar copias de seguridad del contenido de una sola tabla de una base de datos, de varias tablas de una base de datos o de toda la base de datos de CA Service Desk Manager mediante la utilidad de copia de seguridad `pdm_backup`. La salida de dicha utilidad consiste en un archivo ASCII susceptible de uso por parte de la utilidad `pdm_restore`.

como parte de su procesamiento, la utilidad `pdm_backup` cierra primero los demonios (UNIX) o los servicios (Windows).

Más información:

[pdm_backup: escritura de bases de datos en archivos ASCII](#) (en la página 1007)

Restauración de la base de datos

La utilidad de restauración de bases de datos, `pdm_restore`, carga archivos de salida de `pdm_backup` en las bases de datos de CA Service Desk Manager. La utilidad `pdm_restore` primero cierra los daemons (UNIX) o servicios (Windows). Luego restaura, borra y reemplaza todos los registros existentes de las bases de datos. La utilidad `pdm_restore` emplea como entrada el archivo ASCII con formato creado por la utilidad `pdm_backup`.

Las utilidades `pdm_restore` y `pdm_userload` permiten, asimismo, obtener acceso a la aplicación CA Service Desk Manager en caso de que se dañen por completo las bases de datos. Si la base de datos se daña hasta tal punto de que no se pueda obtener acceso a la aplicación y fallen todas las demás medidas previstas, vuelva a ejecutar la configuración y reinicie la base de datos a fin de regenerarla e introducir los datos de referencia y las tablas del sistema.

Con este procedimiento se inicia la base de datos del mismo modo que se hizo durante la instalación original. Ahora tendrá acceso ahora a CA Service Desk Manager. La utilidad `pdm_restore` sirve para restaurar la última copia de seguridad de la base de datos.

Más información:

[pdm_restore: restauración de bases de datos](#) (en la página 1039)

Reemplazo de la tabla de base de datos

La utilidad `pdm_replace` ofrece un modo fácil y rápido de reemplazar todo el contenido de una tabla de la base de datos de CA Service Desk Manager por nueva información. Esta utilidad puede resultar útil para las revisiones masivas de las tablas de-búsqueda.

Nota: La utilidad `pdm_replace` usa el mismo formato de archivo de entrada que la utilidad `pdm_userload`. Es posible crear un archivo de entrada para la utilidad `pdm_replace` por medio de la utilidad `pdm_extract`, pero no se puede emplear como entrada la salida de la utilidad `pdm_backup`.

Más información:

[Cómo crear y utilizar un archivo de entrada](#) (en la página 449)

[pdm_replace: reemplazo de tablas de bases de datos](#) (en la página 1037)

Extracción de datos

La utilidad `pdm_extract` sirve para extraer datos de las bases de datos de CA Service Desk Manager y producir salidas con diferentes formatos. A continuación, estos datos se someten a un ulterior procesamiento o se introducen en otras aplicaciones, como hojas de cálculo u otras bases de datos.

Con la utilidad `pdm_extract`, puede hacer lo siguiente:

- Vuelque la base de datos de CA Service Desk Manager completa
- Volcar una o más de las tablas de las bases de datos
- Extraer información específica de las bases de datos y producir una salida con uno de estos tres formatos:
 - Salida compatible con `pdm_userload`
 - Salida en archivo de valores separados por comas-(CSV)
 - Salida en estilo-de informe informal

Más información:

[pdm_extract: extracción de datos de las bases de datos](#) (en la página 1019)

Uso de la utilidad de extracción de datos en UNIX

Antes de emplear la utilidad de extracción de datos de CA Service Desk Manager en UNIX, realice estos pasos:

1. Defina el valor de la variable de entorno `$NX_ROOT` en la ruta completa al directorio de instalación de CA Service Desk Manager definida durante la instalación.
2. Agregue `$NX_ROOT/bin` a la variable de entorno `PATH`.
3. Defina `umask` en `000`.

Selección de datos para la extracción

Con objeto de seleccionar los datos pertinentes para la extracción, esta utilidad usa un subconjunto SQL integral con las siguientes reglas:

- En el subconjunto se admiten de forma específica estas funciones SQL:
 - `IS NULL`, `IS NOT NULL`, `LIKE`
 - Instrucciones `SELECT` y cláusulas `WHERE`
- En el subconjunto no se admiten estas funciones SQL:
 - Uniones
 - Caracteres de nueva-línea y fichas incrustadas
 - Otras cláusulas aparte de `SELECT`, `FROM` y `WHERE`
 - Asteriscos (*) en las instrucciones `SELECT`
 - Instrucciones `SELECT` anidadas
 - Funciones de adición
- Todas las palabras reservadas de SQL se deben escribir en mayúscula.
- Todos los símbolos de las cláusulas `WHERE` deben llevar espacio delante y detrás.

- Todas las especificaciones de fecha u hora se deben realizar siguiendo uno de estos tres formatos:

- Segundos transcurridos desde las 12:00:00 a. m. de 1/1/1970, hora del meridiano de Greenwich (GMT):

`start_date< o >174182431500`

- Formato SQL DATE:

`start_date< o >DATE '2001-11-28'`

- Formato SQL TIMESTAMP:

`start_date< o >TIMESTAMP '2001-07-04 15:45:00'`

Nota: El formato TIMESTAMP se rige por el horario GMT. Puede ajustar las zonas horarias agregando o restando el número apropiado de horas, como: 2001-03-23 14:00:00+02:00 ó 2001-06-06 04:45:00-09:00.

Anulación de referencias a datos

La utilidad `pdm_deref` es una herramienta de anulación de referencias que convierte datos de diversas fuentes a un formato apropiado para cargarse en la base de datos de CA Service Desk Manager. La anulación de referencias extrae los ID internos para los campos de referencia-cruzada. También se puede emplea para calcular los períodos de inactividad así como los valores de estos períodos que atañan a los acuerdos de nivel de servicio.

La utilidad `pdm_deref` convierte los datos a uno de los formatos siguientes:

- Salida compatible con `pdm_userload`, apta para la carga en las bases de datos de CA Service Desk Manager
- Salida en archivo de valores separados por comas-(CSV)
- Salida en estilo-de informe informal

Más información:

[pdm_deref: anulación de referencias de datos ASCII](#) (en la página 1011)

Ejemplo de cómo utilizar pdm_deref

El ejemplo siguiente muestra cómo utilizar la utilidad `pdm_deref` en un sistema de seguimiento de tickets de CA Service Desk Manager.

Supongamos, por ejemplo, que el sistema de seguimiento de partes implementado en una hoja de cálculo dispone de las columnas Descripción del problema, Nombre y apellidos del técnico y Fecha de entrada. Tales columnas se corresponden con los campos de descripción, asignatario y `open_date` de la tabla `Change_Request` de CA Service Desk Manager. El campo Descripción del problema contiene el mismo tipo de datos que el campo de descripción, pero el campo de asignatario es numérico, en tanto que el campo Técnico de la hoja de cálculo tiene el formato "apellidos, nombre".

Para utilizar pdm_deref

1. Cargue los nombres de los técnicos en la tabla Contacto.
2. Prepare un archivo de entrada de `pdm_deref` con la información existente.
3. Construya un archivo de especificaciones para asignar los nuevos nombres de contacto a valores de asignatario.
4. Prepare un archivo de entrada de `pdm_userload` para ser utilizado con el propósito de actualizar la tabla `Change_Request`.

Este proceso se describe con más detalle en los pasos siguientes:

1. Prepare un archivo de entrada de `pdm_userload`, `location.dat`, para la tabla `Location` del modo siguiente:

```
TABLE ca.location
location_name address_2 address_2
{"Boulder NCC - NQ", "716 Main
    Street", "Boulder, CO 84302"}
{"Colorado Springs NCC", "2765 Spring Street",
    "Colorado Springs, CO 84303"}
{"Denver NCC", "3765 Stoneridge Way", "Denver,
    CO 80254"}
```

2. Cargue los datos con este comando:

```
pdm_load -f location.dat
```

3. Prepare un archivo de entrada, `contact.dat`, con la información original como se ilustra a continuación:

```
TABLE ca.contact
last_name first_name middle_name location pri_phone_number
{"Harrison", "Frank", "Harold", "NCC - HQ", "303-555-2333"}
{"Hertzog", "William", "I.", "Colorado Springs NCC", "303-966-1987"}
{"Lyman", "Jeanie", "L.", "Denver NCC", "303-966-5301"}
```

4. Prepare un archivo de especificaciones para la herramienta de anulación de referencias, `contact.spec`, de la siguiente manera:

```
Deref
{
input = c_location
output = location_uuid
rule = "SELECT id FROM ca.location WHERE location_name=?"
}
```

Importante: no deje ningún espacio en blanco delante de la palabra clave `SELECT`. La utilidad se sirve de los nombres y los apellidos de los nuevos contactos para obtener los campos de ID numéricos apropiados para cargar la tabla `Change_Request`. Además, los “enlaces” representados por medio de signos de interrogación (?) se corresponden con los campos de entrada especificados. Es preciso disponer del mismo número de enlaces que de campos de entrada, y en el mismo orden.

5. Ejecute `pdm_deref` de la siguiente manera:

```
pdm_deref -s contact.spec < contact.dat > contact.out
```

El archivo de salida, `contact.out`, es similar a la secuencia siguiente:

```
TABLE ca.contact
last_name first_name middle_name location.uuid pri_phone_number
{"Harrison", "Frank", "Harold", "69499D5A2424884887E62EC9823F5E47",
"303-555-2333"}
{"Hertzog", "William", "I.", "86873FA40BA4234A8CF7A418D7C8B2DB",
"303-966-1987"}
{"Lyman", "Jeanie", "L.", "58AA42789957734E8BEE146D07F7AD49", "303-966-5301"}
```

6. Cargue el archivo `contact.out` en la base de datos de CA Service Desk Manager como se detalla a continuación:

```
pdm_load -i -f contact.out
```

Nota: Para utilizar la opción `-i`, es necesario usar el comando `pdm_load`.

7. (UNIX solamente, opcional) Escriba un script, `Convert_Ticket`, como se muestra a continuación:

```
#!/bin/sh
pdm_load -i $1
cat $2 | pdm_deref -s $3 | pdm_load -i
```

Para ejecutar esta secuencia de comandos, escriba lo siguiente:

```
Convert Ticket location.dat contact.dat contact.spec
```

En este ejemplo, se emplea `pdm_load` con el indicador `-i` para agilizar el proceso. Si se efectúan estas actualizaciones de manera periódica, conviene omitir el indicador `-i` para que `pdm_load` compruebe si existen registros duplicados.

A continuación, se presentan algunos otros ejemplos de archivos de especificaciones de la herramienta de anulación de referencias:

```
deref
{
    input = first_name, last_name, middle_name
    output = assignee
    rule = " SELECT id from ca.contact \

            WHERE first_name=? \
            AND last_name=? \
            AND middle_name=? "
}
```

Esta regla sirve para convertir tres campos llamados first_name, last_name y middle_name en el UUID del contacto apropiado. Deben estar presentes los tres campos de entrada para que se aplique la regla. Si no se encuentra ninguna coincidencia, aparece un mensaje de error y continúa el procesamiento. En caso de que haya varias coincidencias, se emplea el primer valor; aparece un mensaje de error y continúa el procesamiento.

Modo dbadmin

El modo dbadmin es una utilidad que inicia la capa de manipulación de datos del sistema CA Service Desk Manager sin iniciar la capa de objetos, ofreciendo la capacidad de cerrar la base de datos completa para realizar el mantenimiento de los datos de bajo nivel sin arriesgar la integridad de los datos.

Por ejemplo, probablemente quiera usar las utilidades pdm_extract, pdm_load, pdm_deref y pdm_replace para realizar actualizaciones de datos por lotes en el sistema, al utilizar dbadmin, coloca un bloqueo en toda la base de datos del sistema. Tanto la utilidad de copia de seguridad (pdm_backup) como la de restauración (pdm_restore) colocan automáticamente el sistema en modo dbadmin para garantizar una copia de seguridad y una restauración coherentes.

El modo dbadmin también resulta útil si quiere personalizar el sistema sin iniciar la capa de objetos hasta que se hayan modificado los datos. Por ejemplo, si se convierte algún atributo de sistemas existentes en "obligatorio" en majic, podría ser motivo de confusión para el animador en caso de que tenga que actualizar algún objeto en el que se haya asignado el valor nulo a dicho atributo. Tiene la posibilidad de colocar el sistema en modo dbadmin, actualizar los objetos por medio de la utilidad pdm_load y, a continuación, iniciar el sistema de la forma habitual.

Para colocar el sistema en el modo dbadmin

1. Detenga CA Service Desk Manager con el administrador de servicios de Windows o ejecutando la utilidad pdm_halt en la línea de comandos.

Nota: Antes de detener el sistema, es recomendable alertar a los usuarios y comprobar que no haya usuarios conectados.

2. En la línea de comandos, escriba el siguiente comando distinguiendo entre mayúsculas y minúsculas:

```
pdm_d_mgr -s DBADMIN
```

Nota: No aparece ningún mensaje, pero sí se produce una pausa antes de que se muestre el símbolo del sistema. Si no se produce ninguna pausa, compruebe si ha escrito de manera correcta el comando.

3. Ejecute la utilidad pdm_status para confirmar que el sistema se encuentra en modo dbadmin.

Nota: Si el sistema se encuentra en modo dbadmin, devuelve el mensaje siguiente, que indica que es seguro trabajar en él:

```
C:\>pdm_status  
Los demonios no están en ejecución.
```

4. Una vez realizadas todas las tareas, ejecute la utilidad pdm_halt para salir del modo dbadmin.
5. Reinicie el sistema siguiendo el procedimiento habitual.

Reglas de archivado y borrado definitivo

Puede definir las reglas que desea utilizar para ejecutar las tareas de archivado y borrado definitivo en la base de datos de CA Service Desk Manager. Puede modificar y activar las reglas existentes en lugar de crear otras.

Nota: Si se está integrando con FAST y los foros o documentos manualmente suprimidos, o usó archivado y borrado definitivo para suprimirlos y se está integrando con FAST, se muestran los registros suprimidos en los resultados de la búsqueda como "No disponible". Estos registros se muestran hasta que CA Service Desk Manager y FAST se sincronicen; lo que toma algunos minutos.

Importante: las reglas de archivado y borrado definitivo predeterminadas se establecen como inactivas. Debe establecer el filtro de búsqueda para buscar reglas inactivas. Puede ejecutar una regla seleccionándola desde el nodo Reglas de archivado y borrado definitivo y haciendo clic en Ejecutar ahora.

Ejemplo: activación de la regla del registro de auditorías

Puede activar y ejecutar la regla para archivar y borrar definitivamente los registros del registro de auditoría.

Para activar la regla del registro de auditoría

1. Desplácese a Archivado y borrado definitivo, Reglas de archivado y borrado definitivo
Aparecerá la lista de reglas de archivado y borrado definitivo.
2. Haga clic en Mostrar filtro.
Seleccione Inactivo en la lista desplegable Estado. Haga clic en Buscar.
Aparecen las reglas inactivas.
3. Seleccione la regla Registro de auditorías y haga clic en Ejecutar ahora.
El proceso de archivado y borrado definitivo empieza para los registros del registro de auditoría.

Nota: Puede editar la regla (see page 462) si hace clic en el vínculo de Registro de auditorías y, después, en Editar.

Ejecución de reglas de archivado y borrado definitivo

Puede ejecutar las reglas de archivado y borrado directo tanto activas como inactivas en el momento que quiera.

Para ejecutar una regla de archivado y borrado definitivo desde la página Lista

1. En la ficha Administración, seleccione Archivado y borrado definitivo, Reglas de archivado y borrado definitivo en el panel de la izquierda.
Aparecerá la lista de reglas de archivado y borrado definitivo.
2. Seleccione las reglas que quiere ejecutar haciendo clic en el cuadro a la izquierda del nombre de la regla. Luego elija el número de horas (1 a 24) después de las cuales quiere que la regla se detenga y haga clic en Ejecutar ahora.
Aparece un mensaje que indica que el proceso de archivado y borrado definitivo ha comenzado.

3. Haga clic en Aceptar para cerrar el cuadro del mensaje.

Para ejecutar una regla de archivado y borrado definitivo desde la página Detalle

1. En la ficha Administración, seleccione Archivado y borrado definitivo, Reglas de archivado y borrado definitivo en el panel de la izquierda.
Aparecerá la lista de reglas de archivado y borrado definitivo.
2. Seleccione la regla deseada haciendo clic en el nombre de la regla.
Aparecerá la página Regla de archivado y borrado definitivo.
3. Elija el número de horas (1 a 24) después de las cuales quiere que la regla se detenga y haga clic en Ejecutar ahora.

Visualización de reglas de archivado y borrado definitivo

Puede ver la información resumida para cada regla de archivado y borrado definitivo en la página Lista de reglas de archivado y borrado definitivo. Para mostrar esta página, seleccione Archivado y borrado definitivo, Reglas de archivado y borrado definitivo en el panel de la izquierda en la ficha Administración.

Puede configurar filtros para que sólo se muestren las reglas que coincidan con ciertos criterios.

Búsqueda de la lista de reglas de archivado y borrado definitivo.

Puede configurar filtros para que sólo se muestren las reglas de archivado y borrado definitivo que coincidan con ciertos criterios.

Para filtrar la lista de reglas de archivado y borrado definitivo

1. Haga clic en Mostrar filtro en la página Lista de reglas de archivado y borrado definitivo.
La parte superior de la página muestra los campos del filtro.
2. Complete los campos como sea necesario para mostrar solamente las reglas de interés.
3. Haga clic en Buscar.

La Lista de reglas de archivado y borrado definitivo muestra las reglas que coinciden con los criterios de filtrado.

Inicio del archivado y borrado definitivo mediante programadores de terceros

Puede utilizar un planificador de terceros para iniciar y detener una regla de archivado y borrado definitivo. El planificador debe admitir la emisión de comandos desde una línea de comandos. El archivo arcpur.frg se encuentra en el siguiente directorio:

```
$NX_ROOT\bopcfg\interp
```

Para iniciar el archivado y borrado definitivo mediante planificadores de terceros

1. Abra el planificador de terceros.
2. Especifique la hora de comienzo.
3. Ejecute el siguiente comando:
`bop_cmd -f arcpur.frg "start_arcpur('<rule_name>')"`
4. Establezca el la hora de finalización.
5. Ejecute el siguiente comando:
`bop_cmd -f arcpur.frg "stop_arcpur('<rule_name>')"`
Se ha programado el archivado y borrado definitivo.

Definiciones de reglas de archivado y borrado definitivo

Puede definir las reglas que desea utilizar para ejecutar las tareas de archivado y borrado definitivo en la base de datos de CA Service Desk Manager. El producto ofrece un conjunto de reglas de archivado y borrado definitivo predefinidas. Puede optar por modificar y activar las reglas existentes en lugar de crear otras.

Creación de una regla de archivado y borrado definitivo

Puede establecer reglas para archivar automáticamente registros desactualizados y borrarlos definitivamente de la base de datos.

Para crear una regla de archivado y borrado definitivo

1. En la ficha Administración, seleccione Reglas de archivado y borrado definitivo.
Aparecerá la lista de reglas de archivado y borrado definitivo.
2. Haga clic en Crear.
Aparecerá la página Crear nueva regla de archivado y borrado definitivo.

3. Rellene los campos como corresponda.
4. Haga clic en Guardar.

La nueva regla aparece en la página Lista de reglas de archivado y borrado definitivo.

Más información:

[Campos de reglas de archivado y borrado definitivo](#) (en la página 462)

[Ejecución de reglas de archivado y borrado definitivo](#) (en la página 459)

Campos de reglas de archivado y borrado definitivo

Puede utilizar los campos de las páginas de reglas de archivado y borrado definitivo para definir y editar las definiciones de regla.

Nombre de regla

(Obligatorio) Especifica un identificador exclusivo para la regla. Puede tener un máximo de 30 caracteres alfanuméricos.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

(Obligatorio) Indica si esta regla está activa o inactiva.

Programación

Especifica un turno en el que debería estar vigente la regla. El administrador es quien define los turnos.

Intervalo de repetición

Especifica la frecuencia con la que se ejecuta esta regla, con el formato horas:minutos:segundos (HH:MM:SS).

Nombre de archivo de almacenamiento

Especifica el nombre del archivo donde desea que se almacenen los registros anticuados. Su ubicación viene determinada por la variable NX_RULE_ARCHIVE_PATH que se encuentra en el archivo NX.env. Los archivos de datos archivados se pueden restaurar a la base de datos mediante la utilidad PDM_LOAD.

Tipo de operación

Especifica uno de los tipos siguientes de operación que debería ejecutar la regla:

Archivar/Borrar definitivamente

Borra definitivamente los registros anticuados de la base de datos escritos en el archivo especificado en el campo Nombre del archivo de archivado.

Sólo depuración

Borra definitivamente los registros anticuados de la base de datos, pero no se escriben en el archivo de archivado.

Sólo archivado (ejecución de prueba)

Escribe los registros anticuados en el archivo de archivado sin borrarlos definitivamente de la base de datos. Utilice esta opción para probar una regla de archivado y borrado definitivo recién creada o editada.

Config. Nombre de objeto

Especifica el nombre del objeto de la base de datos que esta regla puede archivar y borrar definitivamente.

Nombre de objeto

(De sólo lectura) Incluye automáticamente la selección en el campo Config. nombre de objeto.

Días de inactividad

Especifica el número de días que un registro permanece inactivo para que sea apto para el archivado y borrado definitivo de la base de datos.

Consulta adicional

Archiva y borra definitivamente registros inactivos específicos entre los registros inactivos existentes. Utilice este campo cuando desee crear reglas diferentes para archivar o borrar definitivamente los subconjuntos de registros vencidos del mismo objeto. Utilice la misma sintaxis que para las consultas almacenadas.

Por ejemplo, la siguiente consulta almacena y depura únicamente los registros de solicitud inactivos asignados de prioridad 1:

`priority = 1 AND (assignee IS NOT NULL OR group IS NOT NULL) and active = 0`

Edición de una regla de archivado y borrado definitivo

Puede editar una regla de archivado y borrado definitivo que ya se haya creado.

Para editar una regla de archivado y borrado definitivo

1. En la ficha Administración, seleccione Reglas de archivado y borrado definitivo.
Aparecerá la lista de reglas de archivado y borrado definitivo.
2. Seleccione la regla que quiera editar y haga clic en el nombre de la regla.
Aparecerá la página Detalles de regla de archivado y borrado definitivo

3. Haga clic en Editar.
Aparecerá la página Actualizar regla de archivado y borrado definitivo.
4. Edite en los campos según sea necesario.
5. Haga clic en Guardar.
Sus ediciones se guardan, y aparece la página Lista de reglas de archivado y borrado definitivo.

Más información:

[Campos de reglas de archivado y borrado definitivo](#) (en la página 462)

[Ejecución de reglas de archivado y borrado definitivo](#) (en la página 459)

Historial de archivado y borrado definitivo

Puede ver un resumen de la información de historial para cada regla de archivado y borrado definitivo.

Para ver el historial de archivado y borrado definitivo

1. Seleccione Archivado y borrado definitivo, Historial de archivado y borrado definitivo en la ficha Administración.

Aparecerá la lista de historiales de archivado y borrado definitivo. Esta lista muestra una entrada por cada vez que se ejecutó la regla.

2. Se muestran los siguientes campos:

Nombre de regla

Muestra el nombre de la regla utilizada en la lista de historiales.

Hora de inicio

Muestra la hora en la que la regla se inició.

Hora de finalización

Muestra la hora en la que la regla se completó.

Objetos principales borrados definitivamente

Muestra los objetos principales que la regla borró definitivamente. Por ejemplo, una petición de llamada.

Objetos secundarios borrados definitivamente

Muestra los objetos secundarios relacionados que la regla borró definitivamente. Por ejemplo, los registros de actividades de una petición de llamada.

3. (Opcional) Haga clic en Mostrar filtro y especifique criterios de filtrado para limitar la lista a la información de interés.

4. Haga clic en el nombre de una regla si quiere revisar su configuración.
Aparecerá la página Detalles de regla de archivado y borrado definitivo

Filtrado de la lista de historiales de archivado y borrado definitivo

Puede filtrar la lista de historiales de archivado y borrado definitivo para mostrar solamente las entradas de interés.

Para filtrar la lista de historiales de archivado y borrado definitivo

1. Seleccione Mostrar filtro en la página Lista de historiales de archivado y borrado definitivo.

La parte superior de la página muestra los campos de filtrado.

2. Complete los campos como sea necesario para mostrar las entradas que quiere ver:

Nombre de regla

Seleccione el nombre de la regla de archivado y borrado definitivo cuyo historial quiere ver.

Primera fecha de inicio

Introduzca la primera fecha y hora a fin de especificar el inicio de un intervalo para filtrar el historial con el propósito de que muestre solamente las entradas que corresponden a un marco de tiempo especificado.

Última fecha de inicio

Introduzca la última fecha y hora a fin de especificar el inicio de un intervalo para filtrar el historial con el propósito de que muestre solamente las entradas que corresponden a un marco de tiempo especificado.

Primera fecha de finalización

Introduzca la primera fecha y hora a fin de especificar el final de un intervalo para filtrar el historial con el propósito de que muestre solamente las entradas que corresponden a un marco de tiempo especificado.

Última fecha de finalización

Introduzca la última fecha y hora a fin de especificar el final de un intervalo para filtrar el historial con el propósito de que muestre solamente las entradas que corresponden a un marco de tiempo especificado.

Nota: Para mostrar el campo Argumentos de búsqueda adicionales, haga clic en el icono de llave. Este campo está dirigido únicamente a usuarios avanzados que conocen SQL y Majic, y que pueden usarlos para especificar argumentos de búsqueda que no están disponibles en los campos de filtro de búsqueda estándar. Para especificar un argumento de búsqueda adicional, introduzca una cláusula WHERE de SQL en este campo.

3. Haga clic en Buscar.

La página Lista de historiales de archivado y borrado definitivo muestra las entradas que coinciden con los criterios de filtrado.

Gestión de adjuntos (arcpur)

Se guardan registros de adjunto en la base de datos y se guardan archivos de adjunto en el directorio del repositorio. Cuando archive y borre definitivamente los registros de adjuntos en la base de datos, se marcarán como suprimidos, pero no podrán eliminarse. Estos registros son necesarios para que el daemon del repositorio pueda localizar los adjuntos.

Configuración del tipo de archivo

Puede configurar el tipo de archivo en relación con los adjuntos de un repositorio desde la ficha Administración.

Procedimiento para configurar el tipo de archivo

1. Vaya a la Biblioteca de adjuntos, Repositorios.
Aparecerá la página Repositorios.
2. Haga clic con el botón derecho del ratón en un repositorio (como Service Desk) y seleccione Ver.
Aparecerá la página Detalles del repositorio.
3. Haga clic en Editar.
Seleccione una de las siguientes opciones en la lista desplegable Tipo de archivo:

Ninguno

No se ejecuta ningún proceso de archivado y borrado definitivo.

Archivado y borrado definitivo

Los registros anticuados se escriben en el archivo especificado en el campo Nombre del archivo de archivado y se borran definitivamente de la base de datos.

Sólo depuración

Los registros anticuados se borran definitivamente de la base de datos, pero no se escriben en el archivo de archivado.

4. Haga clic en Guardar.

Aparecerá la página Detalles del repositorio, con los cambios.

Nota: No puede utilizar el archivado y borrado definitivo con Gestión del conocimiento. Sólo CA Service Desk Manager es compatible con esta función.

Configuración de la ruta de archivo

Puede configurar la ruta de archivo para los adjuntos de la ficha Administración.

Para configurar la ruta de archivo

1. Vaya a la Biblioteca de adjuntos, Repositorios.

Aparecerá la página Repositorios.

2. Haga clic con el botón derecho del ratón en un repositorio (como Centro de servicio al usuario), seleccione Ver.

Aparecerá la página Detalles del repositorio.

3. Haga clic en Editar.

Introduzca la ruta en el campo Ruta de archivo.

El siguiente es el directorio predeterminado:

`$NX_ROOT/site/attachments/default/archived_files`

4. Haga clic en Guardar.

Aparecerá la página Detalles del repositorio, con los cambios.

Cómo restaurar datos archivados

Al restaurar datos archivados, debería iniciar los daemon en el modo dbadmin con la utilidad pdm_d_mgr. El modo dbadmin permite acceso limitado, para que pueda ejecutar con seguridad pdm_load para restaurar los datos archivados.

A continuación se describe cómo se restauran los datos archivados:

1. Cierre CA Service Desk Manager.
2. Inicie los daemon en el modo dbadmin utilizando el siguiente comando:

```
pdm_d_mgr -s DBADMIN
```
3. Localice el archivo de datos archivado. De manera predeterminada, el archivo está ubicado en \$NX_ROOT/site/data/archive.
4. Ejecute pdm_load comparándolo con el archivo de datos. Por ejemplo:

```
pdm_load -a -f 2004611T1726_Call_Request.dat
```
5. Si hay un problema con la carga, revise la línea de comandos y el registro en busca de errores. Se pueden encontrar archivos Arcpur.log en \$NX_ROOT/log.

Nota: Las limitaciones de tamaño de los archivos arcpur.log se definen en \$NX_ROOT/NX.env de la siguiente manera

```
# El límite de tamaño para el archivo de registro de Archivado y borrado  
definitivo y el archivo de datos.  
@NX_ARCPUR_FILESIZE=2000000000
```

Archivado y borrado definitivo crea arcpur.log.0, y arcpur.log.1 a arcpur.log.9 después de haber alcanzado el límite de archivo para cada archivo de registro.

6. Ejecute pdm_halt.
Esto cierra los daemon.
7. Reinicie CA Service Desk Manager.
Nota: Después de haber restaurado el registro, se archiva y se borra definitivamente en el ciclo siguiente del proceso de archivado y borrado definitivo.
8. (Opcional) Para prevenir que el registro se archive y borre definitivamente en el ciclo siguiente, haga lo siguiente:
 - a. Actualice el registro para hacerlo activo otra vez.
 - b. Desactive la regla de archivado y borrado definitivo.

Archivado y borrado definitivo de datos de KPI

Existen reglas de archivado y borrado definitivo predefinidas disponibles para archivar y borrar definitivamente datos de KPI. Vaya a Archivado y borrado definitivo, Reglas de archivado y borrado definitivo en la ficha Administración. Luego, filtre la lista buscando reglas inactivas. Puede seleccionar una de las reglas siguientes y establecerla como activa:

- KPI_Data(SQL)
- KPI_Data(Consulta almacenada)

- KPI_Data(Sistema)
- KPI_Ticket_Data

Se puede crear una regla de configuración opcional dentro de los archivos arcpur_cfg.xml e itil_arcpur_cfg.xml para archivar y borrar definitivamente la tabla KPI_Ticket_Data.

Puede encontrar los archivos en los siguientes directorios:

- arcpur_cfg.xml
\$NX_ROOT\site\cfg\
- itil_arcpur_cfg.xml
\$NX_ROOT\site\cfg\

Utilice los métodos siguientes para archivar y borrar definitivamente la tabla KPI_Ticket_Data:

Tabla KPI_Ticket_Data

- Utilice end_time (last_mod_dt) en KPI_Ticket_data para determinar si un registro necesita archivar y borrarse definitivamente.
- Vincule los registros de la tabla KPI_Ticket_Data con los registros de la tabla Ticket (como cr, chg o iss). Esto garantiza que todos los registros de ticket relacionados de la tabla KPI_Ticket_Data se archiven y borren definitivamente.

La tabla KPI_Ticket_Data no tiene una relación SREL con ninguna tabla Ticket y confía en dos campos, obj_name y obj_id, para vincularse con un ticket. El valor de obj_name puede ser cr, chg o iss y el valor de obj_id es el ID del ticket. Defina un objeto main_obj para cada objeto de ticket.

A continuación se brinda una definición de muestra de main_object para el objeto de ticket, cr:

```
<!-- KPI Ticket Data -->
<main_obj>
<name>KPI Ticket Data</name>
<internal_name>KPI Ticket Data</internal_name>
<factory>ktd</factory>
<default_query>obj_name='cr'</default_query>
<date_field>end_time</date_field>
<ref_by value="obj_id">cr.id</ref_by>
</main_obj>
```

Nota: La regla de configuración puede seleccionar solamente registros para cr. La etiqueta ref_by puede hacer coincidir el valor de obj_id en KPI Ticket Data con valor del ID en cr. Si se encuentra alguna coincidencia, significa que hay un registro de KPI Ticket Data al que hace referencia un registro de cr, por lo que no se archivará ni borrará definitivamente el registro de KPI Ticket Data.

Después de haber agregado las reglas de configuración para todos los objetos de ticket, reinicie el servicio de CA Service Desk Manager. Estas reglas de configuración se convierten en nombres de objetos de configuración seleccionables en el formulario Detalles de regla de archivado y borrado definitivo.

Foros de Gestión del conocimiento de archivado y borrado definitivo

Puede utilizar reglas de archivado y borrado definitivo para eliminar foros suprimidos de la base de datos. Puede crear reglas de archivado y borrado definitivo para archivar y borrar definitivamente sólo documentos del tipo foro.

Nota: Si no crea ninguna regla de archivado y borrado definitivo, la regla de documentos de conocimiento existente puede archivar y borrar definitivamente todos los documentos eliminados, incluidos los documentos del tipo foro.

Para crear una regla para foros de archivado y borrado definitivo

1. Vaya a Archivado y borrado definitivo, Reglas de archivado y borrado definitivo en la ficha Administración.

Aparecerá la lista de reglas de archivado y borrado definitivo.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nueva regla de archivado y borrado definitivo.

3. Realice lo siguiente:

- Seleccione "documento de conocimiento" en la lista desplegable Config. nombre de objeto.
- Agregue "KS_TYPE=20" al campo Consulta adicional.

4. Haga clic en Guardar.

Se crea la nueva regla de archivado y borrado definitivo.

Archivado y borrado definitivo con FAST ESP

Después de archivar y borrar definitivamente tickets, ejecute `pdm_k_reindex` para sincronizar FAST ESP con los registros suprimidos. De lo contrario, estos registros se muestran como no disponibles en la UI.

Ejemplo: Ejecución de `pdm_k_reindex` para sincronizar FAST ESP con incidencias eliminadas

Ejecute el siguiente comando:

```
pdm_k_reindex sync factory:iss
```


Capítulo 12: Uso del API de texto

Esta sección contiene los siguientes temas:

[API de texto](#) (en la página 473)

[El archivo de configuración](#) (en la página 487)

API de texto

Text API es una interfaz que le permite utilizar entradas de texto para crear y actualizar objetos de la base de datos de CA Service Desk Manager como, por ejemplo, incidencias, solicitudes, contactos y activos. Utilizando el API de texto puede asignar valores a la mayor parte de los campos que son accesibles para los usuarios.

Importante: CA Service Desk Manager exige que todas las entradas tengan el formato UTF-8. De lo contrario, pueden corromperse. La utilidad `pdm_unconv` (see page 1045) le permite convertir los datos de un conjunto de caracteres local a UTF-8 y viceversa.

Puede accederse al API de texto mediante las siguientes interfaces:

- Línea de comandos
- Correo electrónico
- CA NSM

Nota: Para la integración entre aplicaciones puede utilizar los servicios Web en lugar del API de texto.

Más información:

[Métodos de conversión](#) (en la página 485)

Interfaz de línea de comandos

El comando `pdm_text_cmd` se emplea para activar la interfaz de la línea de comandos del API de texto. Puede especificar determinada información, por ejemplo, la tabla que debe procesarse y la operación que debe realizarse por medio de parámetros en el comando `pdm_text_cmd`.

La entrada del API de texto se traslada al comando `pdm_text_cmd` con la forma de un archivo de entrada o directamente desde STDIN.

Más información:

[pdm_text_cmd: interfaz de la línea de comandos de Text API](#) (en la página 1042)

Interfaz de CA Network and Systems Management

Cuando se han integrado CA NSM y CA Service Desk Manager, y se crean peticiones desde eventos de CA NSM, el parámetro `user_parms` de las definiciones de reglas de escritura se traslada al API de texto. El proceso de escritura de CA Service Desk Manager (tngwriter) define sus propios parámetros de reemplazo para cambiar el texto antes de enviarlo a Text API. La palabra clave `LOG_AGENT` se agrega al final de la entrada para establecer el `log_agent` para la petición.

Nota: Necesita actualizar el archivo `Text_API.cfg` para todos los campos adicionales que se trasladan desde los sistemas de gestión de alertas de CA NSM a CA Service Desk Manager. Este archivo se utiliza para integraciones con servicios Web, correo electrónico y AHD.DLL.

Más información:

[Palabras clave](#) (en la página 476)

Formato de entrada

La entrada al API de texto se especifica de las siguientes maneras:

- En la interfaz de línea de comandos, la entrada se especifica generalmente en un archivo de texto pasado al comando `pdm_text_cmd`.
- En la interfaz de correo electrónico, se especifica en el texto del correo electrónico. El usuario especifica una expresión regular para encontrar los identificadores de objeto de destino.

El usuario aplica formato a la entrada del API de texto de la misma manera sin importar qué interfaz utiliza.

El formato básico para la entrada es el siguiente:

`%palabra_clave=valor`

or

`%PROPERTY={{etiqueta_propiedad}}valor`

El comportamiento normal de los comandos del API de texto tiene las excepciones siguientes, donde el comando que aparece al último de dos o más comandos en conflicto tiene prioridad:

- Cuando un mensaje contiene varios artefactos de ID de ticket válidos que coinciden con la cadena de filtro de regla de buzón de correo o varios comandos de ID de ticket del API de texto, se utiliza el primero que se encuentra. También, un artefacto de ID de ticket, que se identifica utilizando la cadena de filtro de regla para el buzón de correo, anula cualquier comando de ID de ticket del API de texto, sin tener en cuenta cuál aparece primero.
- Cuando un mensaje contiene varios comandos del API de texto de comentario del registro, todos los comentarios se envían, aunque el orden en el cual aparecen en el registro de actividades del ticket puede variar.

Todos los artefactos de ID de ticket que coinciden con el filtro, sean válidos o no, y los comandos de ID de ticket del API de texto dentro del mensaje, sean aplicables o no, o se hayan aplicado o no, se comentan antes de que el mensaje se envíe. Los artefactos de ID de ticket identificados a través de los filtros de la regla para el buzón de correo aparecen como -((...))- . Los signos de porcentaje (%) adelante de los comandos de ID del API de texto se convierten en dos paréntesis de apertura ((, y dos paréntesis de cierre)) siguen al comando. Si un comando de ID de ticket del API de texto aparece después de otro comando del API de texto con un comentario de registro (%LOG=...), el comando de ID de ticket del API de texto comentado se convierte en un comentario de registro separado.

Nota: El comentario de registro es el único comando del API de texto que puede aparecer repetidas veces en un mensaje y aún así tener cada resultado aplicado. Para algunos otros comandos, el API de texto utiliza solamente el último resultado porque los resultados múltiples de otros comandos se contradicen. Los comandos de comentario de registro múltiples envían mensajes de comentario de registro separados al ticket, y no necesariamente siguiendo algún orden en particular.

Además, si un comando de ID de ticket del API de texto aparece en el mensaje, ya sea al inicio del mensaje o entre otros dos comandos del API de texto, se convierte en un comentario de registro. Si el comando anterior es un comentario de registro (%LOG=...) o una descripción de actualización (%DESCRIPTION=...), se añade a ese comando en lugar de convertirse en un comentario de registro separado.

Los mensajes entrantes que se envían sólo como HTML, sin una versión de texto sin formato incluida, pierde su cuerpo de mensaje. Si el mensaje hace coincidir algunos filtros de regla para el buzón de correo con un cuerpo de mensaje vacío, se puede crear un ticket con una descripción vacía o con el asunto de mensaje citado como la totalidad de la descripción de ticket.

Palabras clave

Hay dos tipos de palabras clave que se pueden utilizar en las entradas de Text API.

- Definiciones en la sección [KEYWORDS] del archivo text_api.cfg: este tipo es un grupo de palabras clave relacionadas directamente con los campos de diversas tablas que se pueden actualizar. Por ejemplo, en esta sección se definen la mayoría de los campos del formulario Detalles de incidencia. Con estas palabras clave, es posible definir valores para los campos de los registros que se estén actualizando o creando. Por ejemplo, la línea siguiente define la prioridad de una incidencia en 5:

```
%PRIORITY=5
```

La sección [KEYWORDS] del archivo text_api.cfg lista todas las palabras clave. Puede definir palabras clave adicionales (por ejemplo, para permitir el acceso del API de texto a campos que ha agregado al personalizar su esquema de base de datos).

- Las siguientes palabras clave especiales se definen siempre de la siguiente manera, sin tener en cuenta el contenido del archivo text_api.cfg:

Palabra clave	Descripción
ASSET	Se emplea para adjuntar elementos a los tickets; es válida para peticiones, incidencias y órdenes de cambio. El valor especificado es el nombre del elemento, que ya debe existir. Esta palabra clave se puede especificar varias veces ya que los tickets pueden tener adjuntos varios elementos.
ATTACHMENT	La interfaz de correo electrónico la usa de forma interna para agregar adjuntos a los partes.
DESCRIPTION	Especifica el valor que se debe usar para el campo de descripción del parte. Esta palabra clave se sobrentiende si se envía la entrada a Text API sin indicar ninguna palabra clave. Esta palabra clave es aplicada automáticamente por el receptor de correo cuando el mensaje no empieza con una palabra clave pero contiene un artefacto de ID de ticket o palabra clave. Es posible cambiar la manera de tratar en las actualizaciones la palabra clave DESCRIPTION mediante la entrada siguiente de la sección [OPTIONS] del archivo text_api.cfg: <pre>UPDATE_DESC_IS_LOG</pre> Si se define esta opción en SÍ, se emplea el valor para crear un comentario de registro; en cambio, si se define en NO, el valor sobrescribe el campo de descripción existente.
FROM_EMAIL FROM_EMAIL_OVERRIDE	La interfaz de correo electrónico la usa para realizar la comparación con el campo Dirección de correo electrónico del registro de la tabla

Palabra clave	Descripción
	ca_contact. También sirve como log_agent para el tíquet. Si se proporcionan los dos, se ignora FROM_EMAIL. Nota: El receptor de correo establece FROM_EMAIL automáticamente por el receptor con la dirección del remitente del mensaje.
FROM_PERSID	La interfaz de la línea de comandos la usa para definir el log_agent de las operaciones, por ejemplo, si el registro de ca_contact carece de ID de usuario. pdm_text_cmd traslada automáticamente esta palabra clave si se especifica el parámetro -p. El valor se compara con el valor de persistent_id del registro de ca_contact.
FROM_USERID	Sólo se usa en la interfaz de la línea de comandos para definir el log_agent de las operaciones. pdm_text_cmd traslada automáticamente esta palabra clave si se especifica el parámetro -u. El valor se compara con el ID de usuario de un contacto.
LOG	Sirve para crear entradas de registro; es válida para solicitudes, órdenes de cambios, incidencias y contactos. El receptor de correo aplica esta palabra clave automáticamente cuando el mensaje no empieza con una palabra clave pero contiene o un artefacto de ID de ticket o palabra clave, o una palabra clave DESCRIPTION.
LOG_AGENT	La interfaz de CA NSM la usa para definir el log_agent de las operaciones. El valor se compara con el campo ID del registro de contacto oportuno.
PROPERTY	Sirve para definir el valor de las propiedades; es válida para solicitudes, órdenes de cambios e incidencias. A diferencia de otras palabras clave, que van seguidas tan sólo de un signo igual y un valor, la sintaxis de la palabra clave PROPERTY debe incluir la etiqueta de la propiedad como se ilustra a continuación: PROPERTY={{etiqueta_propiedad}}valor Debe especificar la <i>etiqueta_propiedad</i> exactamente como aparezca en la base de datos.
SEARCH	Sólo se usa en la interfaz de la línea de comandos y la interfaz de CA NSM para suministrar una lista de palabras clave que se pueden usar en las consultas para actualizar varios tickets para un activo. El valor se corresponde con la lista de palabras clave que se emplea en la búsqueda. La interfaz de CA NSM define de forma automática la palabra clave SEARCH.
SEARCH_EXPLICIT	Sólo se usa en la interfaz de CA NSM para sustituir la palabra clave SEARCH que proporciona la propia interfaz. Los valores aportados son idénticos a los de la palabra clave SEARCH.

Más información:

[pdm_text_cmd: interfaz de la línea de comandos de Text API](#) (en la página 1042)

Convenciones de entrada de palabra clave

Se aplican las siguientes convenciones para aplicar formato a la entrada de palabras clave:

- Coloque un prefijo en todas las palabras clave (incluso PROPERTY) con un signo de porcentaje (%). El signo de porcentaje debe estar en la posición de columna uno. Si la primera línea no vacía de la entrada no tiene un signo de porcentaje en el principio de la línea, se usa %DESCRIPTION= o %LOG= como prefijo para los datos entrantes, dependiendo de si se encontró una palabra clave o un artefacto de ID de ticket. Si se establece %DESCRIPTION, el contenido del mensaje hasta la primera palabra clave se envía como una descripción de ticket. Si se establece %LOG=, el contenido del mensaje hasta la primera palabra clave se envía como un comentario de registro.
- No introduzca ningún espacio entre la palabra clave y el símbolo %, ni tampoco entre la palabra clave y el signo igual (=).
- No entrecomille los valores: se supone que todos los datos que siguen al signo igual son valores.
- Las palabras clave no distinguen entre mayúsculas y minúsculas.
- Si la entrada incluye palabras clave duplicadas, se utiliza la última palabra clave. De lo contrario, el orden en el cual especifica los pares de palabra clave/valor es insignificante.
- Especifique los valores de las palabras clave del mismo modo que en los campos correspondientes en la interfaz Web. Por ejemplo, para indicar un tipo de contacto de analista, debe usar %CONTACT_TYPE=Analista aunque, en la base de datos, dicho valor se almacene como un entero. En text_api.cfg se define la palabra clave CONTACT_TYPE para que convierta el valor especificado (see page 485) de manera que coincida con el valor almacenado.
Nota: Que el valor distinga mayúsculas de minúsculas depende del DBMS subyacente.
- Los datos de cadena pueden abarcar varias líneas.

Cómo dar formato a un mensaje de correo electrónico para actualizar un ticket

Un usuario puede aplicar formato a un mensaje de correo electrónico para crear o actualizar un ticket.

Para aplicar formato a un mensaje de correo electrónico para crear o actualizar un ticket, utilice los campos siguientes:

A

Especifica el nombre del buzón de correo asignado al contacto de CA Service Desk Manager configurado para el usuario privilegiado.

Desde

Especifica la persona que envía el correo electrónico. Se debe definir a la persona en la tabla `ca_contact` a menos que, en la regla para el buzón de correo aplicable, se haya especificado la opción Permitir anónimo.

Nota: La dirección de origen generalmente es parte de la configuración de su programa de correo electrónico y normalmente no se establece en forma individual para cada mensaje.

Adjuntos

Agrega documentos y otros archivos al correo electrónico para enviarle adjuntos al API de texto.

Asunto

Hace coincidir palabras clave en una cadena de filtro de la regla para el buzón de correo, especialmente cuando se crea un ticket.

Cuerpo

Especifica el cuerpo del mensaje de un correo electrónico que usa el API de texto. Puede especificar la palabra clave `ISSUE_ID`, `REQUEST_ID` o `CHANGE_ID`, según el tipo de ticket para crear o actualizar un ticket.

Inicio y finalización de delimitadores de mensaje de correo electrónico

Algunas interfaces de correo electrónico agregan información al principio o al final de los mensajes de correo, lo que puede provocar un funcionamiento incorrecto de la interfaz de correo electrónico (por ejemplo, la codificación MIME). Si su interfaz de correo electrónico agrega información, puede utilizar los siguientes delimitadores: `start-request` y `end-request`. La interfaz de correo electrónico ignora toda la información que se especifique antes de `start-request` y después de `end-request`.

Nota: El receptor de correo no admite correos electrónicos en los formatos RTF o sólo HTML.

Ejemplo: uso de los delimitadores start-request y end-request

```
"start-request"  
cuerpo_mensaje  
"end-request"
```

Cómo utiliza artefactos el API del texto

El API de texto procesa el asunto o el cuerpo de las notificaciones por correo electrónico. Las reglas para el buzón de correo le permiten identificar artefactos y valores que el API de texto utiliza. Por ejemplo, puede definir la regla para incidentes como Incident:{{object_id}}, para que al encontrar Incident:1234 traduzca a %INCIDENT_ID=1234 para el API de texto. 1234 es el ref_num para el incidente. Porque el artefacto debe ser único en el correo electrónico y debe poder encontrarse fácilmente, puede hacer que se diferencie más como por ejemplo %Incident:{{object_id}}%.

Coloque detrás de la palabra clave {{object_id}} un carácter que no sea una letra, un número, una coma, una barra diagonal (/), el signo más (+) ni el signo igual (=), porque estos caracteres pueden aparecer dentro de un artefacto. De lo contrario, es posible que los caracteres que siguen al artefacto puedan ser malinterpretados como parte del valor del artefacto, o que un carácter dentro del valor del artefacto se pueda malinterpretar como el carácter que sigue al valor.

El receptor de correo realiza lo siguiente:

1. Busca el artefacto dentro de un correo electrónico (como Incident:1234) que asigna al ticket apropiado u otro objeto compatible con el API de texto.
2. Traduce el artefacto a un token del API de texto (como %INCIDENT_ID=1234).
3. Envía el mensaje etiquetado al API de texto. El API de texto procesa el correo electrónico, aplica el texto, los comandos o ambos que contienen al ticket apropiado y genera un correo electrónico de respuesta automática que indica si el mensaje de correo electrónico que recibió se aplicó correctamente. Dependiendo de las acciones ejecutadas, también se envía un mensaje de correo electrónico de notificación por separado para indicar ciertos eventos específicos, como la creación de un ticket.

Cómo configurar respuestas de notificación para actualizar tickets.

El daemon de Text API (pdm_text_nxd) crea y actualiza tickets con información de interfaces externas, como la línea de comandos y el correo electrónico. Puede configurar el correo para que utilice Text API de modo que los usuarios (contactos) puedan actualizar tickets respondiendo a notificaciones de correo electrónico. El texto de la respuesta se agrega como actividad de comentario de registro al ticket.

Si desea configurar respuestas de notificación para actualizar tickets, realice lo siguiente:

1. Establezca el método de notificación que utiliza el contacto en `pdm_mail -T reply_email_address` o `pdm_mail -F reply_email_address`. La opción `reply_email_address` especifica la dirección entrante para el buzón de correo. Cuando el contacto hace clic en Respuesta en un correo electrónico, esa dirección se rellena desde la dirección del remitente o respuesta del mensaje al que está respondiendo.

-T establece la dirección de respuesta. -F establece la dirección del remitente, que se utiliza como dirección de respuesta si no se especifica una distinta.

Nota: Algunos programas de correo no aceptan direcciones de respuesta.

2. Cree o actualice una regla para el buzón de correo mediante una palabra clave de Text API.

Los artefactos definidos por el usuario en los filtros de la regla para el buzón de correo reemplazan a las siguientes palabras clave de Text API:

Objeto	Palabra clave de Text API	Identificador
Incidente	%INCIDENT_ID	Ref_num
Problema	%PROBLEM_ID	Ref_num
Solicitud	%REQUEST_ID	Ref_num
Chg_ref_num	%CHANGE_ID	Chg_ref_num
Incidencia	%ISSUE_ID	Ref_num

3. Cree o actualice una frase de notificación que coincida con la regla.
4. Cree o actualice una plantilla de mensaje que utilice la frase de notificación.
5. Actualice la regla de buzón de correo creada en el paso 2 para especificar la plantilla de mensaje creada en el paso 4.

Nota: Para obtener información sobre cómo llevar a cabo cada paso, consulte la *Ayuda en línea*.

Después de que el usuario recibe la notificación y la responde, se producen las siguientes acciones:

1. Cuando se encuentra la cadena de filtro, la palabra clave de ID de ticket relevante y el valor indicado por el marcador de posición, de haberlos, se añaden al mensaje.
2. Si se encuentra un artefacto de ID de ticket coincidente, el ticket correspondiente se actualiza, ya sea con un comentario de registro, una nueva descripción u otros valores de acuerdo con el texto, las palabras clave y los comandos en el mensaje.
3. Si no se encuentra un artefacto de ID de ticket coincidente, se crea un ticket con una descripción y otros parámetros de acuerdo con el texto, las palabras clave y los comandos en el mensaje.

Cómo configurar una respuesta en un ejemplo de notificación de incidente.

Este ejemplo muestra cómo configurar una respuesta en una notificación de incidente.

Para configurar una respuesta en una notificación de incidente, realice lo siguiente:

1. Cree una regla para el buzón de correo con los siguientes campos y valores:
 - Filtro: el cuerpo contiene
 - Cadena de filtro: %Incident:{{object_id}}%
 - Omitir mayúsculas y minúsculas: SÍ
 - Acción: actualizar objeto
 - Objeto de acción: incidente
2. Cree una frase de notificación que incluya la siguiente regla:
 - Símbolo: respuesta de incidente
 - Código: respuesta de incidente

- Activo: activo
- Descripción: comentario que incrusta la respuesta para un incidente/problema/solicitud.
- Frase: para agregar un comentario a `@{call_req_id.type.sym}`, conteste este correo o incluya la línea siguiente (en una sola línea).

`%Incident:{call_req_id.ref_num}%`

Nota: En el texto de respuesta automática de la regla para el buzón de correo, omita el prefijo `call_req_id`. Este prefijo aplica un contexto en el que ya se encuentra el texto de la regla para el buzón de correo; dicho cambio de contexto no es válido cuando ya actúa dentro de ese contexto.

3. Cree o actualice una plantilla de mensaje que utilice la siguiente frase de notificación:

- Cuerpo del mensaje de notificación

Esto es una simple notificación.
`@{notification_phrase[IncidentURL1].phrase}`

4. Actualice la regla de buzón de correo creada en el paso 1 para especificar la plantilla de mensaje creada en el paso 3, de la siguiente forma:

Plantilla de mensaje: *nombre de la regla para el buzón de correo*

Cómo actualizan ejemplos de ticket los usuarios finales

El siguiente ejemplo demuestra cómo responde un usuario final (Juan Pérez) a una notificación por correo electrónico para actualizar un ticket de incidentes.

El cuerpo o el asunto del correo electrónico incluye el identificador de objeto. El marcador de posición `{{object_id}}` dentro de la cadena de filtro indica el identificador de objeto.

1. Se envía una notificación a Juan Pérez que incluye las siguientes instrucciones:

Para agregar un comentario al incidente, conteste este correo o incluya la línea siguiente (en una sola línea).

`%Incident:1234%`

2. Juan Pérez responde a la notificación de la siguiente manera:

Ésta es mi respuesta...

3. El receptor de correo recibe la versión de texto siguiente del correo electrónico de Juan Pérez:

Ésta es mi respuesta...

De: Centro de servicio al usuario

Enviado: miércoles 18 de septiembre de 2009, 10:22

A: Pérez, Juan

Tema: Simple notificación

Esto es una simple notificación.

Para agregar un comentario al incidente, conteste este correo o incluya la línea siguiente (en una sola línea).

%Incident:1234%

4. El receptor de correo procesa las reglas en orden y encuentra el artefacto **%Incident:1234%**:

Ésta es mi respuesta...

De: Centro de servicio al usuario

Enviado: miércoles 18 de septiembre de 2009, 10:22

A: Pérez, Juan

Tema: Simple notificación

Esto es una simple notificación.

Para agregar un comentario al incidente, conteste este correo o incluya la línea siguiente (en una sola línea).

%INCIDENT_ID=1234

5. El receptor de correo agrega las palabras clave de API de texto y el valor **{{object_id}}** a una declaración **%INCIDENT_ID=** y deja un marcador donde se encontró el valor **{{object_id}}**. El siguiente texto muestra los datos que se envían al API de texto. El texto en negrita muestra los valores agregados por el receptor de correo.

%LOG=Ésta es mi respuesta...

De: Centro de servicio al usuario

Enviado: miércoles 18 de septiembre de 2009, 10:22

A: Pérez, Juan

Tema: Simple notificación

Esto es una simple notificación.

Para agregar un comentario al incidente, conteste este correo o incluya la línea siguiente (en una sola línea).

%Incident:-(...)-%

%FROM_EMAIL=juan.perez@compañía.com

%INCIDENT_ID=1234

6. El API de texto agrega un comentario de registro para el incidente 1234.

Métodos de conversión

Muchas de las palabras clave definidas en el archivo `text_api.cfg` cuentan con un método asociado que permite convertir el valor especificado en el valor apropiado para el almacenamiento en la base de datos. Esta función permite a los usuarios especificar valores del mismo modo que se hace en la interfaz Web, sin necesidad de que tengan conocimientos de la implementación subyacente.

El archivo de configuración tiene varios ejemplos de este tipo de definición de la palabra clave, incluyendo `ISSUE.PRIORITY` y `CONTACT.CONTACT_TYPE`. Si necesita definir más palabras clave (por ejemplo, para permitir que el API de texto acceda a campos que haya agregado al personalizar su esquema de base de datos), puede utilizar uno de los siguientes métodos predefinidos:

Método	Tipo de salida
<code>lookup_actbool</code>	INTEGER
<code>lookup_asset_by_name</code>	UUID
<code>lookup_asset_by_persid</code>	UUID
<code>lookup_chg_category</code>	CADENA
<code>lookup_chg_status</code>	CADENA
<code>lookup_cnt_by_email</code>	UUID
<code>lookup_cnt_by_last_first_middle</code>	UUID
<code>lookup_cnt_by_logonid</code>	UUID
<code>lookup_cnt_by_persid</code>	UUID
<code>lookup_cnt_meth</code>	INTEGER
<code>lookup_cnt_type</code>	INTEGER
<code>lookup_company</code>	UUID
<code>lookup_cr_status</code>	CADENA
<code>lookup_cr_template</code>	CADENA
<code>lookup_domain</code>	INTEGER
<code>lookup_grc</code>	INTEGER
<code>lookup_group</code>	UUID
<code>lookup_impact</code>	INTEGER
<code>lookup_iss_category</code>	CADENA
<code>lookup_iss_status</code>	CADENA

Método	Tipo de salida
lookup_loc	UUID
lookup_mfr_model	UUID
lookup_nr_family	INTEGER
lookup_org	UUID
lookup_person_contacting	INTEGER
lookup_position	INTEGER
lookup_priority	INTEGER
lookup_prob_category	CADENA
lookup_product	INTEGER
lookup_resource_status	INTEGER
lookup_service_lvl	CADENA
lookup_severity	INTEGER
lookup_state	INTEGER
lookup_timezone	CADENA
lookup_type_of_contact	INTEGER
lookup_urgency	INTEGER
lookup_workshift	CADENA

Si ninguno de los métodos anteriores es apropiado para el valor que se debe convertir, es necesario escribir un método personalizado. El método debe tomar un valor de CADENA como entrada y devolver otro valor (ENTERO, CADENA o UUID) como salida. Si se devuelve el valor -1 (o "-1"), se denota que el valor no se puede determinar y que, por consiguiente, no está definido. En el caso de UUID, se devuelve un valor nulo.

Por ejemplo, es posible desarrollar un método que convierta el ID de usuario en una referencia de la tabla ca_contact. El valor entrante, Administrador, por ejemplo, se traslada al método, que devuelve el ID de la tabla ca_contact correspondiente al ID de usuario del administrador.

La manera de definir las palabras clave en el archivo de configuración ofrece la ventaja de poder definir varias asignaciones de palabras clave para el mismo campo, incluidos diferentes métodos de conversión, en función del valor especificado. Por ejemplo, los asignatarios pueden tener varias asignaciones distintas de palabras clave que indiquen cómo se define su valor según los diversos valores de entrada. Las entradas pueden corresponder al ID de usuario, a los apellidos, al nombre o al segundo nombre y también al ID real de `ca_contact` (por ejemplo, `793ED69B4E87A545BD8E911834D829FC`). Cada una de las palabras clave se asigna a un método de conversión diferente, salvo el último, que no necesita someterse a ninguna conversión.

El archivo de configuración

En el archivo `text_api.cfg` se definen las palabras clave que guardan una relación directa con los campos de las diversas tablas que se pueden actualizar. Este archivo se emplea con dos fines: por un lado, como referencia para la búsqueda de determinados valores predefinidos, como las palabras clave y, por otro, como mecanismo para la configuración del API de texto, si bien el archivo de configuración predeterminado funciona a la perfección con la mayoría de las instalaciones sin que haga falta introducir ninguna modificación.

El archivo `text_api.cfg` se encuentra en el siguiente directorio:

- UNIX: `$NX_ROOT/site`
- Windows: `installation-directory\site` Por ejemplo: `C:\Archivos de programa\CA\Service Desk\site`

El archivo de configuración está dividido en secciones, en cada una de las cuales se definen determinados atributos. Las definiciones de atributos adoptan el formato siguiente:

```
palabra_clave=valor
```

En ninguna de las palabras clave se realiza la distinción entre mayúsculas y minúsculas pero sí en los valores (salvo en la sección `[OPTIONS]`).

Nota: Puede ver y modificar el archivo `text_api.cfg` usando cualquier editor de texto.

Importante: si se está integrando con el componente Sistemas de gestión de alertas de CA NSM, debe actualizar `text_api.cfg` para todo campo adicional que se traslade a CA Service Desk Manager.

Más información:

[Palabras clave](#) (en la página 476)

Opciones

En la sección [OPTIONS] del archivo text_api.cfg se definen opciones de procesamiento que pueden diferir de un sitio a otro. Así, por ejemplo, contiene opciones que determinan el formato de las fechas entrantes, los campos que permiten conservar los saltos de línea o el permiso para actualizar las incidencias, las solicitudes o las órdenes de cambios con la interfaz de correo electrónico. Todas las opciones de esta sección son susceptibles de configuración. Tenga en cuenta que, aunque es posible eliminar nombres de tablas de VALID_TABLE_LIST, si no desea que se admita el acceso de Text API a dichas tablas, no se pueden agregar nombres de tablas a la lista.

Valores predeterminados

En el archivo text_api.cfg, hay varias secciones [..._DEFAULTS], una por cada interfaz que emplee el API de texto, por ejemplo, [EMAIL_DEFAULTS] para la interfaz de correo electrónico o [CMD_DEFAULTS] para la interfaz de la línea de comandos. En estas secciones se definen los valores predeterminados de los campos y las propiedades necesarios en caso de que los usuarios no los proporcionen directamente.

Para definir los valores predeterminados, utilice uno de los formatos siguientes:

- nombre_tabla.palabra_clave=valor

La *palabra_clave* se debe definir en la sección [KEYWORDS] o como propiedad en la base de datos oportuna. El método asociado a la palabra clave se aplica de manera automática al *valor*. Por ejemplo:

ISSUE.PRIORITY=1

La palabra clave PRIORITY se define en el archivo text_api.cfg para que realice una búsqueda con el propósito de convertir el valor especificado para que coincida con el valor correspondiente almacenado en la base de datos. Aquí, el valor 1 se convierte a 5, que es el valor de la base de datos subyacente para el símbolo de prioridad 1. Esta función permite al usuario especificar el valor del mismo modo en que lo haría en la interfaz Web.

- nombre_tabla.**PROPERTY**={{etiqueta_propiedad}}valor

La *etiqueta_propiedad* se debe definir como propiedad en la base de datos oportuna.

En ambos formatos, el *nombre_tabla* debe ser uno de los valores definidos por medio de VALID_TABLE_LIST en la sección [OPTIONS], por ejemplo, Issue, Request o Contact.

Más información:

[Métodos de conversión](#) (en la página 485)

Omisión de entradas

Existen varias secciones [..._IGNORE_INCOMING] en el archivo `text_api.cfg`, una por cada interfaz que emplee el API de texto, por ejemplo, [TNG_IGNORE_INCOMING] para la interfaz de CA NSM y [EXT_IGNORE_INCOMING] para la interfaz externa que usan otros productos de CA. En estas secciones se definen los campos y las propiedades que se omiten en la entrada. El formato es idéntico al de los valores predeterminados salvo en que no se especifica ningún “=valor”. Esta opción le permite impedir que los usuarios establezcan ciertos valores, lo que a su vez, le proporciona más seguridad para ocasiones tales como cuando se permite a los usuarios que utilicen la interfaz de correo electrónico.

Las secciones IGNORE funcionan a la perfección cuando se usan junto con las secciones [..._DEFAULTS] correspondientes porque, al tiempo que se impide al usuario el establecimiento de algún valor, se está suministrando un valor predeterminado que lo sustituye. Por ejemplo, para impedir que los usuarios de la interfaz de correo electrónico definan la prioridad de las incidencias, se podrían definir estos valores:

```
[EMAIL_DEFAULTS]
ISSUE.PRIORITY=2
[EMAIL_IGNORE_INCOMING]
ISSUE.PRIORITY
```

En este caso, se omite la prioridad que especifique el usuario en el cuerpo del mensaje, sea cual sea, y a todas las incidencias creadas mediante la interfaz de correo electrónico se les asigna automáticamente la prioridad 2.

Entrada de ejemplo

En los siguientes ejemplos se muestran entradas que puede utilizar en el cuerpo de un mensaje de correo electrónico o en un archivo que sirva como entrada de la interfaz de línea de comandos.

Ejemplo: la primera línea no incluye ninguna palabra clave

En este ejemplo, como en la primera columna de la primera fila falta una %keyword, se agrega el literal %DESCRIPTION= al principio del mensaje. Esta adición establece el campo de descripción a "Este texto se incluye en el campo de descripción" (con el salto de línea intacto puesto que ISSUE.DESCRPTION se incluye en la lista de campos presente en la entrada LINEFEEDS_ALLOWED de la sección [OPTIONS] del archivo `text_api.cfg`).

```
Este texto se incluye
en el campo de descripción
%PRIORITY=Ninguno
```

Ejemplo: la primera línea incluye una palabra clave

En este ejemplo, la palabra clave **PRIORITY** se define en el archivo `text_api.cfg` para que realice una búsqueda para convertir el valor especificado en el valor correspondiente almacenado en la base de datos. Aquí, el valor **Ninguno** se convierte a 0, que es el valor de la base de datos subyacente para el símbolo de prioridad 1. Esta función permite al usuario especificar el valor igual que en la interfaz Web.

```
%description=Ésta es mi descripción
%priority=Ninguno
%CATEGORY=Actualización.PC
%PROPERTY={{CPU actual}}266 MHz
%PROPERTY={{Disco duro actual}}1 GB
%PROPERTY={{Actualización solicitada}}4 GB disco duro
```

Los valores especificados se emplean para definir los campos de descripción y prioridad del parte, de modo similar al ejemplo anterior (fíjese en que no importa si la palabra clave se escribe con mayúscula o con minúscula).

En cuanto al valor de **Actualización.PC**, éste se busca y se define el campo de categoría del parte en consecuencia.

Cuando se encuentren las etiquetas siguientes, se definen los tres valores de las propiedades:

- CPU actual
- Disco duro actual
- Actualización solicitada

Capítulo 13: Cómo gestionar el control de versión

Nota: En este capítulo, la mayoría de las referencias a los "clientes" se aplican a los clientes o a los servidores secundarios.

Esta sección contiene los siguientes temas:

[Cómo funciona el control de versiones](#) (en la página 491)

[Archivos de control de versión](#) (en la página 492)

[Archivos de control del servidor primario](#) (en la página 492)

[Archivos de control de cliente y de servidor secundario](#) (en la página 493)

[Control de versión para personalizaciones de instalaciones](#) (en la página 493)

[Modos de los servidores para el control de versión](#) (en la página 494)

[Sintaxis de los archivos de control de versión](#) (en la página 496)

Cómo funciona el control de versiones

La función de control de versión de CA Service Desk Manager ayuda a gestionar las personalizaciones del sistema que afectan a los clientes y a los servidores secundarios. Puede utilizar la función de control de versiones en las instalaciones de cliente y de servidor secundario.

El control de versiones funciona de la siguiente manera:

1. Cuando el cliente se conecta al servidor, el cliente envía al servidor una lista de los componentes controlados.
2. El servidor compara entonces esa lista con su propia lista principal.
3. Si el servidor detecta alguna diferencia, puede hacer lo siguiente:
 - Notificar al cliente.
 - No aceptar la conexión.
 - Actualizar el cliente a la versión correcta de los componentes controlados.

Nota: El control de versión no es un sistema de entrega de software; la función de actualización tan sólo brinda un método para corregir problemas poco importantes de sincronización entre los clientes y los servidores.

Archivos de control de versión

CA Service Desk Manager mantiene dos conjuntos de archivos de control de versiones. uno para los servidores secundarios y otro para todos los clientes. Los componentes controlados pueden representar archivos, directorios o el archivo de variables de entorno `client_nx.env`. Los componentes también pueden ser genéricos, es decir, pueden no estar asociados a ningún objeto externo. Los componentes genéricos se pueden utilizar para ofrecer el control de versión a los clientes como un todo, o bien, a archivos o directorios demasiado grandes para admitir la actualización automática. Si las versiones de los componentes genéricos no coinciden, no se actualizan de forma automática. Una incompatibilidad siempre tiene como resultado un error de cliente y debe solucionarse manualmente.

Archivos de control del servidor primario

El control de versión del servidor de CA Service Desk Manager consiste en un archivo ejecutable, `pdm_ver_nxd`, y dos archivos de control de versión, `server_default.ver` y `server_secondary.ver`. La opción de los servidores `ver_ctl` determina el modo en el que el control de versión responde a las discrepancias entre las versiones de los componentes instalados en los servidores y los clientes. La definición predeterminada de la opción del gestor de opciones `ver_ctl` es `ACTUALIZAR`, lo que hace que el control de versión se actualice cuando se detecta una discrepancia.

El ejecutable `pdm_ver_nxd` valida los mensajes de solicitud de versión de los clientes comparando los datos de la solicitud con los siguientes archivos de control de versión:

- `server_default.ver`
- `server_secondary.ver`
- `server_custom.ver`
- `server_secondary_custom.ver`

Si `pdm_ver_nxd` detecta alguna discrepancia en las versiones de los componentes, registra un mensaje con el problema y, como está activado el valor `ACTUALIZAR`, se actualiza el cliente oportuno. El contenido del mensaje de notificación depende del valor de la opción `ver_ctl`.

Si quiere, puede crear y mantener los siguientes dos archivos de control de versión *personalizados* para gestionar personalizaciones:

- `server_secondary_custom.ver`
- `server_custom.ver`

Archivos de control de cliente y de servidor secundario

El control de versión en los servidores secundarios o los clientes de CA Service Desk Manager consiste en un ejecutable (pdm_ver) y un archivo de control de versión (secondary.ver). Si se desea, se puede crear y mantener un segundo archivo de control de versión para gestionar las personalizaciones: server_secondary_custom.ver.

El software cliente incluye un ejecutable, pdm_ver, y un archivo de versión predeterminado, default.ver. La control de versiones crea automáticamente un segundo archivo de versión (custom.ver) en el cliente si existe un archivo server_custom.ver en el servidor. Ambos archivos de versión de los clientes realizan un seguimiento de las versiones tanto de los componentes estándar como de los personalizados que estén instalados en los clientes.

La definición predeterminada de la opción del gestor de opciones ver_ctl es ACTUALIZAR, lo que hace que el control de versión actualice el servidor secundario cuando se detecte una discrepancia. La comprobación de las versiones se lleva a cabo sólo en el caso de servidores secundarios y de clientes remotos; no hace falta realizarla en los clientes que se ejecuten en el servidor primario puesto que éste contiene las copias principales de todos los componentes. El control de versión siempre se efectúa en comparación con el servidor principal. Al iniciar cualquier servidor secundario o cualquier cliente, lee sus archivos de versión y envía un mensaje al servidor principal con una lista de todos los componentes instalados junto con sus versiones. Si hay una discrepancia entre versiones de componentes, el servidor determina su respuesta comprobando la configuración de la opción ver_ctl. La respuesta del servidor insta al cliente a continuar, finalizar o actualizar sus componentes.

Nota: La mayoría de los clientes recibe una descarga de archivos y variables de opciones al iniciar por primera vez. que reflejan las opciones elegidas por el administrador al configurar el servidor e instalar las opciones.

Control de versión para personalizaciones de instalaciones

Después de personalizar los clientes de CA Service Desk Manager, el control de versión permite supervisar y controlar la instalación de las personalizaciones de los clientes. Para ello, es preciso crear un archivo server_custom.ver (server_secondary_custom.ver en el caso de los servidores secundarios) donde se describan las personalizaciones.

El control de versión usa los dos archivos de versión (`server_default.ver` y `server_custom.ver`) de manera independiente cuando pretende verificar la versión de los componentes de los clientes. Los componentes deben estar diseñados de modo que un archivo nunca esté controlado por dos o más componentes. El control de versiones procesa cada componente por separado. El control de versión verifica los archivos cada vez que encuentra algún componente que los controle, lo que produce resultados inesperados a veces si el número de versión o la fecha no son iguales.

Si desea utilizar el control de versiones para supervisar y controlar la instalación de las personalizaciones en los clientes, realice los pasos siguientes:

1. Cree el archivo `server_custom.ver` en una de las siguientes ubicaciones:
 - Linux: `$NX_ROOT/site/mods/server_custom.ver`
 - Windows: `installation-directory\site\mods\server_custom.ver`
2. Agregue un componente a `server_custom.ver` por cada uno de los cambios realizados con una de estas configuraciones:
 - Cree componentes `dir_ctl` para implementar el control de versión en los directorios. Al hacerlo, todos los archivos del directorio en cuestión se consideran de la misma versión y se actualizan al mismo tiempo. Esta configuración reduce al mínimo el mantenimiento de `server_custom.ver` aunque, en ocasiones, se actualizan archivos del cliente que ya estaban actualizados.
 - Cree componentes `file_ctl` para implementar el control de versión en los archivos. Esta configuración ofrece una documentación y un control mejores, pero el archivo `server_custom.ver` puede ser de mayor tamaño.
3. Actualice el número de versión en `server_custom.ver` cada vez que realice un cambio a un componente personalizado. El número de versión permite que el control de versiones reconozca a los clientes que tienen una versión diferente.

Modos de los servidores para el control de versión

La opción de los servidores `ver_ctl` determina el modo en el que el control de versión responde a las discrepancias entre las versiones de los componentes instalados en los servidores y los clientes. Esta opción se define mediante el gestor de opciones.

La opción `ver_ctl` puede tener uno de los siguientes valores:

NOTIFICAR

(Cliente de Windows) Solicita al usuario que continúe o salga si se detecta alguna discrepancia entre las versiones.

(Cliente de Linux) Registra una discrepancia entre versiones, pero el cliente siempre realiza la inicialización. No se cambia ningún archivo para corregir la discrepancia.

ERROR

Termina el cliente si detecta alguna discrepancia entre versiones. Se impide a los usuarios que empleen CA Service Desk Manager hasta que se actualice manualmente el cliente.

DESACTIVAR

Ignora las discrepancias entre versiones. Todos los clientes pueden conectarse.

Nota: Los clientes pueden definir su propia opción `ver_ctl` con el valor `DESACTIVAR` si se desea omitir el control de versión.

ACTUALIZAR

Solicita al cliente que actualice los componentes afectados a la versión correcta si detecta alguna discrepancia entre versiones. Si la actualización se realiza correctamente, la conexión del cliente continúa; en caso contrario, el cliente termina. El método de actualización depende del tipo de control de versión del componente.

Éstos son los valores válidos:

Valor	Descripción
<code>dir_ctl</code>	El cliente agrega archivos al directorio, actualiza archivos o bien elimina archivos de él según las copias que proporciona el servidor. Nunca se elimina el directorio en sí.
<code>file_ctl</code>	El cliente agrega un archivo al directorio, lo actualiza o bien lo elimina de él según la copia que proporciona el servidor.
<code>nxenv_ctl</code>	El cliente actualiza el archivo <code>NX.env</code> .
<code>ver_ctl</code>	Los componentes <code>ver_ctl</code> no se pueden actualizar. Si existen discrepancias en este tipo de componente, se finaliza el cliente sin conectar al servidor.

Sintaxis de los archivos de control de versión

En cada uno de los archivos de control de versión se describen uno o más componentes. Los componentes pueden representar archivos, directorios o el archivo de variables de entorno `client_nx.env`. Los componentes también pueden ser genéricos, es decir, pueden no estar asociados directamente a ningún objeto externo.

Nota: Si desea obtener más información sobre la estructura y la sintaxis de los archivos de control de versión, consulte los archivos `.ver` instalados en el sistema, que se encuentran en el subdirectorio de sitios del directorio de instalación principal de CA Service Desk Manager. Estos archivos contienen comentarios y valores de ejemplo que pueden ser de gran utilidad.

Utilice la sintaxis que se indica más adelante para definir cada uno de los componentes. Los elementos impresos en *cursiva* representan los datos que debe proporcionar. Los parámetros de *nombre-componente* y versión son siempre obligatorios. Algunos de los demás también pueden serlo en función del valor de *tipo-control*. Todos los demás elementos representan palabras clave que se deben escribir exactamente como se muestra en el siguiente ejemplo:

```
[ nombre-componente ]
version = "x.x, yyyymmdd"
tipo-control
filename = "nombre-archivo"
directory = "directorio"
link = "directorio-vínculo"
source = "directorio-origen"
effectivity = "especificación-efectividad"
checksum
min_release = "versión"
max_release = "versión"
component_type = "tipo-archivo"
o_mode = "modo-propietario"
g_mode = "modo-grupo"
w_mode = "modo-genera7"
```

Parámetros de control de versiones

Los siguientes parámetros son aplicables al control de versión:

[**nombre-componente**]

Especifica el nombre del elemento sometido al control de versión. Este nombre debe ser único y debe encerrarse entre corchetes. *nombre-componente* no distingue entre mayúsculas y minúsculas. Este parámetro es obligatorio al principio de la definición de los componentes.

version="x.x. yyymmdd"

Especifica el número (x.x) y la fecha (yyymmdd) que definen la versión de los componentes. Este parámetro es obligatorio y se debe encerrar entre comillas dobles. El control de versión verifica la versión de los componentes comparando el número de versión y la fecha que se guardan en el servidor con el número de versión y la fecha presentes en los clientes. Ambos valores, número de versión y fecha, deben coincidir para que se considere que el componente está sincronizado entre el cliente y el servidor. Si se desea y está activada la propiedad checksum, antes de actualizar el archivo pertinente, se verifica mediante una suma de comprobación.

tipo-control

Especifica el tipo de control de versión del componente. La siguiente configuración es válida para el tipo de control:

Valor	Descripción
dir_ctl	Especifica que el componente representa un directorio. Es preciso aportar el parámetro directory para especificar la ruta de acceso al directorio. También se puede especificar el parámetro filename para especificar una máscara para los archivos del directorio que se debe actualizar en caso de que sea necesaria la actualización. Los subdirectorios no se actualizan ni en UNIX ni en Windows.
file_ctl	Especifica que el componente representa un archivo. Es preciso aportar los parámetros directory y filename para especificar la ruta de acceso al archivo.
nxenv_ctl	Especifica que el componente representa el archivo client_nx.env, que sirve para almacenar variables de entorno internas de CA Service Desk Manager. El control de versión de CA Service Desk Manager y el gestor de opciones automáticamente mantienen este archivo. Existe un solo componente nxenv_ctl cuyo nombre de componente debe ser CLIENT_NXENV.
ver_ctl	Se trata del tipo de control predeterminado. Especifica que el componente es genérico, es decir, que no está asociado a ningún objeto externo. Los componentes genéricos se pueden utilizar para ofrecer el control de versión a los clientes como un todo, o bien, a archivos o directorios demasiado grandes para admitir la actualización automática. Los componentes con el tipo de control ver_ctl no se pueden actualizar. Si las versiones de los componentes ver_ctl no coinciden y el servidor se encuentra en modo ACTUALIZAR, se produce un error en la conexión del cliente.

filename = "nombre-archivo"

Especifica el nombre del archivo sometido al control de versión. No contiene ninguna especificación de directorio. Este parámetro es obligatorio para los componentes file_ctl pero opcional para los componentes de control de directorios (dir_ctl). Si se emplea con los componentes de directorios, el parámetro filename actúa como máscara de archivo que restringe los archivos asociados al componente dir_ctl. Por ejemplo, si el valor de filename para un componente dir_ctl es *.README, la actualización de ese directorio sólo incluye los archivos que terminen por ".README".

directory = "directorio"

Especifica la ruta al directorio en los componentes dir_ctl o al directorio que contiene el archivo en los componentes file_ctl. Este parámetro se ignora en los componentes ver_ctl y nxenv_ctl. La ruta del directorio se debe encerrar entre comillas y puede contener referencias a variables de entorno con el símbolo \$ delante.

Nota: Escriba siempre barras diagonales (no barras inversas) para separar los subdirectorios en los nombres de rutas, incluso en el caso de los servidores de Windows.

link = "directorio-vínculo"

Especifica un directorio de vínculo del cliente en el mismo formato que el parámetro directory. Este parámetro es opcional para los componentes file_ctl y dir_ctl, y se omite en los componentes ver_ctl y nxenv_ctl. Si se especifica, las actualizaciones en los clientes de Linux provocan la colocación de un vínculo simbólico en el directorio de vínculo que señale al archivo copiado en la ubicación especificada por el parámetro directory. Las actualizaciones en los clientes de Windows provocan la copia del archivo tanto en la ubicación de link como en la de directory.

source = "directorio-origen"

(Opcional) Especifica un directorio diferente en el servidor donde éste puede recuperar archivos para la entrega. Tiene el mismo formato que el parámetro directory. Resulta de gran utilidad si los archivos que se deben entregar al cliente son distintos de los archivos de la ubicación de directorio del servidor. Con este parámetro, se insta al servidor a recuperar el archivo del *directorio-origen* y a entregarlo en la ubicación del cliente que especifique el parámetro directory. El parámetro directory es obligatorio si se especifica el parámetro source.

effectivity = "especificación-efectividad"

(Opcional) Especifica si el cliente debe obtener el componente. Permite excluir la descarga a algunos clientes. Los clientes que no estén incluidos en la especificación de efectividad no obtienen el componente. Si se omite este parámetro, todos los clientes reciben el componente. La especificación de efectividad emplea los siguientes símbolos:

+ (signo más)

Indica que se agregue un grupo de clientes.

- (signo menos)

Indica que se excluya un grupo de clientes.

Los grupos de clientes siguientes son válidos:

- SUN4SQL
- AIX
- LINUX
- LINUX390
- HP
- WINDOWS_CLIENTS
- UNIX_CLIENTS

Por ejemplo, la siguiente especificación indica que sólo obtengan los archivos los clientes de UNIX:

```
effectivity = "+ UNIX_CLIENTS"
```

checksum

Instruye al componente a actualizarse si la suma de comprobación del componente del cliente no coincide con la suma de comprobación correspondiente del servidor. Si se aplica a un directorio, la suma de comprobación se aplica a cada uno de sus archivos.

min_release = "versión" y max_release = "versión"

Especifican, respectivamente, los clientes más antiguo y más reciente a los que se deba distribuir el componente. Las instrucciones del archivo `server_default.ver` definen las versiones. Estos parámetros adoptan el formato siguiente, donde GAxx indica la versión y los valores siguientes son valores Genlevel asociados a la versión.

```
! Release GA50 50MvV000900 50w7T000900
! Release GA45 45Mw000900 50wTT000900
```

El orden indica que GA50 es más reciente que GA45.

[nombre-componente]

Especifica el nombre del elemento sometido al control de versión. Este nombre debe ser único y debe encerrarse entre corchetes. *nombre-componente* no distingue entre mayúsculas y minúsculas. Este parámetro es obligatorio al principio de la definición de los componentes.

Valor	Descripción
archivo	Se trata del tipo de componente predeterminado. Especifica que los archivos copiados en el cliente se pueden obtener directamente de la ubicación del servidor que indique el parámetro <code>directory</code> .
exe_file	Especifica que los archivos copiados en el cliente se obtienen de una ubicación del servidor que depende del sistema operativo del cliente, como se muestra a continuación: ■ windows (Windows) ■ sun4Sol (Solaris) ■ hp (HP-UX) ■ aix (AIX) ■ linux (Linux) ■ linux390 (Linux390) Las ubicaciones de estos subdirectorios dependen del valor del parámetro <code>directory</code>. Si se define este parámetro, los subdirectorios se ubican en el <i>directorio</i> indicado. De lo contrario, se ubican en el directorio <code>bin</code> del directorio de instalación principal de CA Service Desk Manager.

o_mode = "modo-propietario"

Especifica los permisos de acceso al archivo del propietario del archivo.

g_mode = "modo-grupo"

Especifica los permisos de acceso al archivo de los usuarios del grupo al que pertenezca el propietario del archivo (sólo se emplea para clientes de UNIX).

w_mode = "modo-general"

Especifica los permisos de acceso al archivo de los usuarios que no estén en el grupo al que pertenezca el propietario del archivo (sólo se emplea para clientes de UNIX).

Los tres parámetros mode permiten el mantenimiento de distintas versiones del mismo ejecutable en el servidor. Especifican controles de acceso al archivo una vez copiado en el cliente. Estos parámetros sólo se utilizan durante las operaciones de actualización. Tienen de uno a tres caracteres con el significado siguiente:

Valor	Descripción
R	Read
W	Escribir
X	Execute

Los equipos cliente ignoran los permisos de escritura y ejecución.

Es posible especificar cualquier combinación de modos de acceso a los archivos. En los clientes de UNIX, se otorga al archivo el modo de acceso especificado. En los equipos cliente, el archivo permite la escritura o es de sólo lectura según se haya especificado o no el parámetro w_mode.

Anulación del control de componentes

En ocasiones, es necesario eliminar el control de ciertos componentes. El problema es que, si se limita a eliminar el componente oportuno del archivo server_default.ver del servidor principal, también se eliminan los archivos asociados. Por ello, es posible definir un bloque para la *anulación del control* en el archivo server_default.ver, lo que facilita la eliminación del componente sin eliminar al mismo tiempo los archivos asociados que hay en los clientes. Las instrucciones pertinentes adoptan el formato siguiente:

```
! uncontrol component-name
```

Esta instrucción indica que el componente debe dejar de estar sometido al control. Los clientes que se conecten al servidor deben eliminar el componente de su archivo de versión y también los archivos asociados al componente. El bloque de anulación de control se puede eliminar una vez que todos los clientes se hayan conectado al menos una vez.

Nota: Es preciso actualizar todos los clientes con el cliente de control de versión más reciente. Los que sean más antiguos pueden ignorar los componentes cuyo control se ha anulado.

Capítulo 14: Gestión de elementos de configuración

Esta sección contiene los siguientes temas:

[Uso de la interfaz Web](#) (en la página 503)
[Elementos de configuración de Contacto, Ubicación y Organización](#) (en la página 508)
[Relaciones CI](#) (en la página 511)
[Control de versiones](#) (en la página 520)
[Visualización de los atributos de un elemento de configuración en otros productos de CA](#) (en la página 548)
[Uso del Visor de CMDB](#) (en la página 549)
[Visualizador CMDB](#) (en la página 549)
[Cómo agregar un activo detectado](#) (en la página 553)
[Indicadores de activo y de CI](#) (en la página 554)
[Conciliación de elementos de configuración](#) (en la página 555)
[Gestión de transacciones guardadas en almacenamiento intermedio](#) (en la página 576)
[Mantenimiento de datos de CA CMDB](#) (en la página 602)

Uso de la interfaz Web

Dependiendo de su rol, puede ejecutar tareas de usuario y administración sobre los elementos de configuración (CI) utilizando las opciones siguientes:

- Los paneles de resultados le permiten ejecutar tareas de usuario y gestionar CI y relaciones de CI.
- La ficha Administración le permite ejecutar tareas de administración con CI y relaciones.
- El Visualizador de CMDB le permite ejecutar tareas de usuario y administración para visualizar CI y relaciones.

Más información:

[Visualización de los elementos de configuración](#) (en la página 504)
[Creación de un elemento de configuración](#) (en la página 504)
[Actualización de un elemento de configuración](#) (en la página 505)
[Cómo asociar una ventana de mantenimiento con un CI](#) (en la página 506)
[Visualización de ventanas asociadas para el cambio](#) (en la página 506)
[Visualización del historial de elementos de configuración](#) (en la página 507)
[Desactivación de un elemento de configuración](#) (en la página 507)
[Reactivación de un elemento de configuración](#) (en la página 508)

Visualización de los elementos de configuración

El panel de resultados permite abrir un elemento de configuración y ver información acerca de él.

Para abrir y ver un elemento de configuración

1. En el panel de resultados, haga clic en Buscar, Elementos de configuración.
Aparecerá el panel Búsqueda de elementos de configuración.
2. Introduzca los criterios de búsqueda y haga clic en Buscar.
Aparecerá la lista de elementos de configuración con los resultados de la búsqueda.
3. (Opcional) Haga clic en un elemento de configuración en la columna Nombre para abrirlo y ver su información detallada.
Aparecen los detalles del elemento de configuración.

Nota: Después de crear un CI, la página de detalles de CI no muestra algunos atributos identificadores si están vacíos (no tienen ningún valor) y no se aplican a la familia de CI. Sin embargo, siempre se muestran los atributos identificadores con valores que no están vacíos.

Creación de un elemento de configuración

El panel de resultados permite crear un elemento de configuración.

Para crear un elemento de configuración.

1. En el panel de resultados, haga clic en Archivo, Nuevo elemento de configuración.
Aparecerá la página Crear nuevo elemento de configuración.
2. Introduzca un nombre exclusivo para el elemento de configuración en el campo Nombre.
3. Introduzca la clase del elemento de configuración en el campo Clase o haga clic en el icono de búsqueda que se encuentra por encima del campo para localizar una clase.
4. Complete el resto de campos aplicables al nuevo elemento de configuración.

Nota: Para crear un elemento de configuración sólo son requeridos los valores de Nombre y Clase.

5. Haga clic en Continuar.
La página Crear nuevo elemento de configuración muestra otros campos y fichas.

6. Introduzca los datos necesarios en los campos apropiados de la ficha Atributos.

Los atributos que aparecen en la ficha se determinan mediante la familia de la clase que se ha seleccionado para el elemento de configuración. La información que introduzca aquí está determinada por los procesos empresariales y por la información que desea almacenar y visualizar para un elemento de configuración.

7. Haga clic en Guardar.

Aparecerá un mensaje que confirma la creación del elemento de configuración.

Nota: Puede generar automáticamente elementos de configuración nuevos y rellenar los atributos utilizando adaptadores de federación incluidos en CA CMDB. Los adaptadores permiten incluir en CA CMDB datos de elementos de configuración de otras fuentes de datos.

Actualización de un elemento de configuración

El panel de resultados permite modificar un elemento de configuración.

Para modificar un elemento de configuración

1. En el panel de resultados, localice y abra el elemento de configuración.

Aparecerá la página de detalles del elemento de configuración.

2. Haga clic en Editar.

Aparecerá la página Actualización del elemento de configuración.

3. Realice cambios en la información del elemento de configuración. Para ello, seleccione las fichas apropiadas en la página e introduzca nuevos datos en los campos. Haga clic en Guardar.

Aparecerá un mensaje que confirma la modificación del elemento de configuración.

Nota: Cuando se actualiza un elemento de configuración con la opción -a, la fecha de última modificación del elemento de configuración y el usuario que aparecen en la lista de elementos de configuración se actualizan aunque no se cambien atributos. Esta actualización se produce si el elemento de configuración se edita en la interfaz de usuario (y se guarda sin cambios) o se actualiza con GRLoader.

Cómo asociar una ventana de mantenimiento con un CI

Para controlar el acceso de mantenimiento a un CI, puede asociar ese CI a una o más ventanas de mantenimiento no globales.

Para asociar una ventana de mantenimiento con un CI

1. Desplácese hasta la página de detalles del elemento de configuración.
2. Haga clic en la ficha Ventanas de mantenimiento.
Aparecerá la lista de ventanas de mantenimiento.
3. Haga clic en Actualización de ventanas de mantenimiento.
Aparece la página Búsqueda de ventanas de mantenimiento.
4. Especifique información para las ventanas de mantenimiento necesarias.
5. Haga clic en Buscar
Aparece la página Ventanas disponibles.
6. Mueva cualquier ventana necesaria de la lista Ventanas para el cambio disponibles a la lista Ventanas para el cambio asociadas.
7. Haga clic en OK.
Se guardan las asociaciones de ventanas nuevas, ventanas para el cambio y el CI.

Visualización de ventanas asociadas para el cambio

Para determinar cómo un CI puede verse afectado durante periodos de tiempo específicos, puede ver las ventanas de mantenimiento que están asociadas con ese CI.

Para ver ventanas para el cambio asociadas con un CI

1. Desplácese hasta la página de detalles del elemento de configuración.
2. Haga clic en la ficha Ventanas de mantenimiento.
Se muestran las ventanas de mantenimiento asociadas.

Visualización del historial de elementos de configuración

Se puede ver el historial de un elemento de configuración.

Para ver el historial de elementos de configuración

1. Busque y abra el elemento de configuración.
Aparecerá la página de detalles del elemento de configuración.
2. Haga clic en la ficha Configurando la versión.
Aparece la página Control de versiones.
3. Haga clic en Mostrar registro.
Se listará el historial de elementos de configuración.
Nota: Mostrar registro ignora las selecciones del panel izquierdo.

Desactivación de un elemento de configuración

Si ya no se va a utilizar un elemento de configuración, es posible editar los detalles del elemento de configuración para desactivarlo. Un estado inactivo suprime el elemento de configuración de la lista de elementos de configuración del panel de resultados. No puede suprimir un elemento de configuración.

Nota: La desactivación de una familia o de una clase no tiene ningún impacto en los CI existentes en dicha familia y clase. Sólo impide la creación de nuevos CI en dicha familia y clase.

Para desactivar un elemento de configuración

1. Busque y abra el elemento de configuración.
Aparecerá la página de detalles del elemento de configuración.
2. Haga clic en Editar.
Aparecerá la página Actualización del elemento de configuración.
3. Seleccione Activo en la lista desplegable Activo. Haga clic en Guardar.
Aparecerá un mensaje que confirma el cambio de estado. El elemento de configuración ya no volverá a aparecer en la lista de elementos de configuración activos. El elemento de configuración continuará apareciendo en las relaciones existentes hasta que se desactiven esas relaciones.

Reactivación de un elemento de configuración

Si es necesario utilizar un elemento de configuración que está inactivo, puede volver a activarlo.

Para volver a activar un elemento de configuración

1. Busque y abra el elemento de configuración.
Aparecerá la página de detalles del elemento de configuración.
2. Haga clic en Editar.
Aparecerá la página Actualización del elemento de configuración.
3. Seleccione Activo en la lista desplegable Activo. Haga clic en Guardar.
Aparecerá un mensaje que confirma el cambio de estado. El elemento de configuración aparecerá en la lista de elementos de configuración activos.

Elementos de configuración de Contacto, Ubicación y Organización

Una instalación de CA CMDB puede definir CI para *objetos base*: Contactos, Ubicaciones y Organizaciones. Estos elementos de configuración se pueden gestionar en conformidad y pueden establecer relaciones con otros elementos de configuración. Para algunos clientes, este enfoque admite de mejor manera el proceso de gestión de la configuración que el uso de objetos base solamente como atributos de CI.

Más información:

[Creación de un CI para un objeto base](#) (en la página 508)
[Selección de un objeto base para un CI](#) (en la página 509)
[Edición de los detalles de un CI para un objeto base](#) (en la página 510)
[Edición de atributos de CI para un objeto base](#) (en la página 510)
[Creación de un CI de objeto base mediante GRLoader](#) (en la página 511)

Creación de un CI para un objeto base

El panel de resultados permite crear un elemento de configuración a partir de un objeto base.

Para crear un CI a partir de un objeto base

1. Haga clic en Archivo, Nuevo elemento de configuración.
Aparecerá la página Crear nuevo elemento de configuración.

2. Rellene los campos del CI. Los campos Nombre y Clase son obligatorios. Haga clic en Continuar.

Nota: Los atributos comunes del CI Nombre de host, Número de serie, Dirección MAC y Nombre de DNS son irrelevantes en un CI para un objeto base.

Aparecerá la página Crear nuevo elemento de configuración.

3. Haga clic en el vínculo del objeto base para definir el objeto que representa este CI.
4. Seleccione el objeto. Se puede buscar un objeto existente o hacer clic en Crear nuevo para crear un objeto. Si quiere crear un objeto, haga clic en Guardar para continuar.

El objeto seleccionado aparecerá en la parte superior de la página Detalles del elemento de configuración.

5. Haga clic en Guardar.

Los atributos principales del objeto seleccionado aparecerán en la ficha Atributos de la página Detalles del elemento de configuración del objeto.

Selección de un objeto base para un CI

Se puede seleccionar un objeto base para un elemento de configuración.

Para seleccionar un objeto base para un CI

1. Seleccione un CI en la familia de objetos base (Contacto, Ubicación u Organización).

Aparecerá la página de detalles del elemento de configuración.

2. Haga clic en Editar.

Aparecerá la página Actualización del elemento de configuración.

3. En la sección superior, complete los campos requeridos para el objeto base. Puede introducir un valor directamente o hacer clic en la lupa para buscar el objeto. Por ejemplo, para buscar un contacto, rellene uno o varios campos de búsqueda en la ventana Búsqueda de contactos y haga clic en Buscar. A continuación, seleccione un contacto en la lista mostrada.
4. Haga clic en Guardar.

Si el objeto seleccionado ya está representado por un CI diferente de la misma familia, aparecerá un mensaje de error. Para poder modificar el CI, debe seleccionar un objeto diferente.

Edición de los detalles de un CI para un objeto base

Es posible editar los atributos del objeto base que representa el CI, por ejemplo ID elem. config. alter. y Notas, del mismo modo que en cualquier otra ventana Detalles del elemento de configuración.

Procedimiento para editar los atributos del objeto base que representa el CI

1. Seleccione un CI en la familia de objetos base.
Aparecerá la página de detalles del elemento de configuración.
2. Haga clic en el vínculo del objeto en la parte superior de la página.
Aparecerá la página de detalles del objeto.
3. Haga clic en Editar.
Aparecerá la página de actualización del objeto.
4. Edite los campos deseados y haga clic en Guardar.
Se cierra la página Actualizar.

Si ha modificado uno de los atributos que aparece en la ficha Atributos de la página Detalles del elemento de configuración, el cambio se mostrará después de actualizar la página.

Edición de atributos de CI para un objeto base

Los atributos del elemento de configuración de un objeto base se pueden modificar.

Para editar los atributos de un CI

1. Seleccione un CI en la familia del objeto (Contacto, Ubicación u Organización).
Aparecerá la página de detalles del elemento de configuración.
2. Haga clic en Editar.
Aparecerá la página Actualización del elemento de configuración.
3. En la ficha Atributos, haga clic en Editar.
Aparecerá la página Actualizar.
4. Edite los campos que desee y haga clic en Guardar.
Se cierra la página Actualizar.
5. Haga clic en Guardar.

La página Detalles del elemento de configuración muestra el CI modificado.

Creación de un CI de objeto base mediante GRLoader

Puede utilizar GRLoader para crear un CI de objeto base a partir de un objeto base existente.

Para utilizar GRLoader para crear un CI de objeto base a partir de un objeto base existente

1. Escriba XML que identifique lo siguiente:

- Nombre de CI
- Familia
- Clase

2. Envíe el XML.

Se crea el objeto base y el GRLoader muestra que se leyó e insertó un CI.

Ejemplo: creación de un CI a partir de un contacto existente

En el siguiente ejemplo se crea un CI a partir del contacto existente **Torres, Juan**.

```
<GRLoader>
<ci>
  <name>Torres, Juan</name>
  <family>Contacto</family>
  <class>Técnico</class>
  <base_contact>Torres, Juan</base_contact>
</ci>
</GRLoader>
```

Relaciones CI

Las funciones de CA Service Desk Manager dependen de las relaciones entre elementos de configuración. Las relaciones de CI tienen las siguientes características:

- El *tipo de relación* define cómo dos elementos de configuración se relacionan.
- Los tipos de relaciones jerárquicas se relacionan como *proveedor/dependiente*. Por ejemplo, A (proveedor) *alberga* a B; B (dependiente) *es albergado por* A.
- Los tipos de relaciones jerárquicas se relacionan como *de punto a punto*. Por ejemplo, *es conectado a*, que es igual en ambas direcciones.

Puede realizar las siguientes funciones de relación utilizando la ficha Relaciones CMDB:

- Ver relaciones activas o inactivas buscando en el campo ¿Activo?
- En la lista relaciones elem. config., puede hacer clic en cualquier vínculo para que una relación inicie su página Detalles de relación entre elementos de configuración.

Más información:

[Tipos de relación entre elementos de configuración](#) (en la página 512)

[Creación de un tipo de relación](#) (en la página 513)

[Gestión de relaciones de CI](#) (en la página 514)

[Creación de relaciones de CI](#) (en la página 514)

[Visualización de las relaciones de un CI](#) (en la página 515)

[Desactivación de relaciones de CI](#) (en la página 515)

[Reactivación de relaciones de CI](#) (en la página 516)

[Desactivación de relaciones de CI \(Editar en lista\)](#) (en la página 516)

[Desactivación de una relación CI mediante GRLoader](#) (en la página 517)

[Reactivación de una relación CI mediante GRLoader](#) (en la página 518)

[Supresión de una relación de CI de la base de datos](#) (en la página 519)

[Comparación e historial de relaciones de CI](#) (en la página 519)

Tipos de relación entre elementos de configuración

CA Service Desk Manager proporciona una lista de tipos de relaciones predefinidos que se pueden utilizar para describir una relación, o asociación, entre elementos de configuración. La forma en que se expresa la relación depende del elemento de configuración central. Por ejemplo, un proveedor *admite* un elemento de configuración dependiente, pero el dependiente es *admitido por* el proveedor. Se trata de diferentes expresiones de la misma relación, y la etiqueta del tipo de relación visualizada depende de si se está viendo una relación de proveedor a dependiente o de dependiente a proveedor.

Nota: Para obtener información sobre los tipos de relaciones que proporciona CA CMDB, consulte la *Referencia técnica de CA CMDB*.

Creación de un tipo de relación

Puede crear un tipo de relación y ponerlo a disposición para crear o actualizar relaciones.

Para crear un tipo de relación

1. En la ficha Administración, amplíe la carpeta de CA CMDB en el panel de la izquierda.
2. Haga clic en Tipos relaciones elem. config.
Aparecerá la lista de tipos de relaciones de elementos de configuración en el panel derecho.
3. Haga clic en Crear nuevo.
Aparecerá la página Crear nuevo tipo de relación entre CI.
4. Rellene los siguientes campos:

Etiqueta proveedor a dependiente

Describe la relación del proveedor al dependiente, y es el nombre que aparece en la lista de tipos de relación. Por ejemplo, "atiende" o "gestiona" es un relación de proveedor a dependiente.

Etiqueta dependiente a proveedor

Describe la relación del dependiente al proveedor, y es el nombre que aparece en la lista de tipos de relación. Por ejemplo, "es atendido por" o "es gestionado por" es una relación de dependiente a proveedor.

De punto a punto?

Especifica que la relación no tiene un CI de proveedor ni un CI dependiente pero, en cambio, consta de dos CI iguales. Por ejemplo, "se conecta a" y "presenta un fallo cuando" son relaciones de punto a punto.

¿Activo?

Pone el tipo de relación a disposición para la selección en relaciones entre elementos de configuración y para que aparezca en listas.

5. Haga clic en Guardar.

Se crea el tipo de relación, y puede utilizarlo para crear o actualizar relaciones.

Gestión de relaciones de CI

La página Relación entre elementos de configuración proporciona todos los valores necesarios en una sola ubicación para simplificar el proceso de relaciones entre elementos de configuración.

Puede utilizar la página para realizar las siguientes acciones:

- Alternar la relación proveedor/dependiente entre dos elementos de configuración.

Haga clic en Revertir para intercambiar el elemento de configuración del proveedor y el elemento de configuración dependiente de la relación. Los CI centrales cambian. Si la relación inversa no es válida, haga clic en el botón Invertir para borrar el campo Relación.

- Establezca campos opcionales como Símbolo, Descripción y Coste.

Haga clic en Opcional para establecer campos opcionales.

Si no se especifica un símbolo, al crear la relación se generará automáticamente un símbolo exclusivo con el prefijo **cmdb bmhier:** y un número exclusivo.

Nota: Si su instalación se integra con CA Network and Systems Management (CA NSM), se le solicitará que especifique el coste y el repositorio de CA NSM.

Creación de relaciones de CI

Es posible agregar una relación de CI a partir de un elemento de configuración central.

Para agregar una relación a partir de un CI central

1. Seleccione el CI al cual desea agregar la relación.
Aparecerá la página Detalles de CI.
2. Haga clic en Editar.
Aparecerá la página Actualizar CI.
3. Haga clic en la ficha Relaciones CMDB y en Crear nuevo.
Aparecerá la página Crear relación de CI.

4. Especifique el elemento de configuración del CI proveedor. Puede hacer clic en el vínculo de lupa para buscar el CI.

Nota: Dependiendo de la relación que quiere, puede hacer clic en Revertir para alternar las posiciones de proveedor/dependiente.

5. Especifique un tipo de relación. Puede hacer clic en el vínculo de lupa para buscar el tipo de relación.
6. Especifique el otro CI (de manera predeterminado, el CI dependiente). Puede hacer clic en la lupa para buscar el CI.
7. Haga clic en Guardar.
Se creará la relación.

Visualización de las relaciones de un CI

Puede ver las relaciones de un CI.

Para ver las relaciones de un CI

1. Desplácese al elemento de configuración.
Aparecerá la página de detalles del elemento de configuración.
2. Seleccione la ficha Relaciones CMDB.
Aparecerá una lista de las relaciones del CI.

Desactivación de relaciones de CI

Puede desactivar una relación de CI estableciendo su estado como Inactivo.

Para desactivar una relación

1. Desplácese a la página Detalles de CI, haga clic en la ficha Relaciones CMDB y luego en Editar.
La ficha Relaciones CMDB se muestra en el modo de edición.
2. Seleccione una relación y haga clic en cualquier vínculo de su fila.
Aparecerá la página Detalles de relación entre elementos de configuración.
3. Haga clic en Editar.
4. Establezca el atributo "¿Activo?" en inactivo. Haga clic en Guardar.
La relación pasa a estar inactiva. En la página Detalles de relación entre elementos de configuración, el atributo "¿Activo?" muestra el valor de atributo Inactivo.

Reactivación de relaciones de CI

Puede reactivar una relación de CI suprimida.

Para reactivar una relación de CI suprimida

1. Desplácese hasta la página de detalles del elemento de configuración.
La página de detalles del CI se muestra en modo de sólo lectura.
2. Haga clic en Editar.
La página de detalles del CI se muestra en modo de edición.
3. Seleccione la ficha Relaciones CMDB.
4. Haga clic en cualquier vínculo de una fila para abrir esa página Detalles de relación entre elementos de configuración.
5. Haga clic en Editar.
Aparecerá la página Actualizar relación entre elementos de configuración.
6. Cambie el atributo "¿Activo?" a "Activo". Haga clic en Guardar.
Se reactivará la relación.

Desactivación de relaciones de CI (Editar en lista)

Puede desactivar una o más relaciones de CI utilizando la función Editar en lista.

Para desactivar una o más relaciones de CI

1. En la ficha Administración, abra la carpeta de CA CMDB en el panel de la izquierda.
El nodo de CA CMDB se expande para mostrar las subcarpetas.
2. Haga clic en la carpeta Lista relaciones elem. config.
3. (Opcional) Especificación de filtros de búsqueda
4. Haga clic en Buscar.
Las relaciones del CI se mostrarán en el panel derecho.
Nota: De forma predeterminada, se muestran todas las relaciones.
5. Haga clic en Editar en lista en la parte superior derecha de la lista.
Se mostrarán los controles de Editar en lista de la relación.

6. Seleccione la fila que contenga la relación que desea modificar.
Se muestra la fila, y los controles se rellenan con los valores de la relación.
7. Establezca el atributo "¿Activo?" en inactivo.
Haga clic en Guardar si quiere desactivar solamente la relación resaltada o haga clic en Cambiar todo si quiere desactivar todas las relaciones en la búsqueda filtrada.

Desactivación de una relación CI mediante GRLoader

Puede desactivar una relación de CI utilizando GRLoader para enviar XML.

Para desactivar una relación mediante GRLoader

1. Escriba XML que utilice una etiqueta de relación para identificar lo siguiente:
 - Elemento de configuración del proveedor
 - Elemento de configuración dependiente
 - Tipo de relación
2. Establezca delete_flag en verdadero (o sí o 1).
3. Envíe el XML.
Se suprime la relación de CI.

Nota: Para obtener información sobre GRLoader, consulte la *Guía de referencia técnica de CA CMDB*.

Ejemplo: supresión de una relación de CI mediante GRLoader

En el siguiente ejemplo de XML, se suprime la relación "conecta a" entre ci_1 y ci_2.

```
<GRLoader>
  <relation>
    <dependent>
      <name>ci_2</name>
    </dependent>
    <type>conecta a</type>
    <provider>
      <name>ci_1</name>
    </provider>
    <delete_flag>true</delete_flag>
  </relation>
</GRLoader>
```

Reactivación de una relación CI mediante GRLoader

Puede reactivar una relación de CI utilizando GRLoader para enviar XML.

Reactivación de una relación de CI mediante GRLoader

1. Escriba XML que utilice una etiqueta de relación para identificar lo siguiente:
 - Tipo de relación
 - Elemento de configuración dependiente
 - Elemento de configuración del proveedor
2. Establezca delete_flag en falso (o no o 0).
3. Envíe el XML.

La relación de CI se reactiva.

Nota: Para obtener más información sobre GRLoader, consulte la *Guía de referencia técnica de CA CMDB*.

Ejemplo: reactivación de una relación de CI

En el siguiente ejemplo de XML, se reactiva la relación "conecta a" entre ci_1 y ci_2.

```
<GRLoader>
  <relation>
    <dependent>
      <name>ci_2</name>
    </dependent>
    <type>conecta a</type>
    <provider>
      <name>ci_1</name>
    </provider>
    <delete_flag>false</delete_flag>
  </relation>
</GRLoader>
```

Supresión de una relación de CI de la base de datos

Puede suprimir una relación de CI para que no sólo se desactive sino también se elimine de la base de datos de forma permanente.

Procedimiento para eliminar una relación de la base de datos

1. Desplácese a la Lista relaciones elem. config.
Aparece la Lista relaciones elem. config.
2. Haga clic con el botón secundario en cualquier fila de relación y seleccione Suprimir.
La relación se elimina de la base de datos.

Importante: si la relación suprimida tiene definido un Símbolo, también se eliminará de la base de datos cualquier relación con el mismo símbolo.

Comparación e historial de relaciones de CI

La ficha Control de versiones muestra relaciones de CI y permite hacer lo siguiente:

- Ver el historial de relaciones de CI para cualquier CI en CMDB. Los cambios realizados en una relación se registran automáticamente al crear, actualizar o suprimir la relación. Puede ver todas las relaciones actuales e históricas para un CI.

Nota: Las relaciones creadas con versiones anteriores de CA CMDB no tienen información del historial de auditoría.

- Compare relaciones en cualquier instantánea o hito.

Control de versiones

El control de versiones fomenta el control de la infraestructura de TI ya que gestiona y hace un seguimiento de los ciclos de vida de todos los CI que constituyen el estado autorizado del CMDB. El control de versiones proporciona las funciones siguientes para controlar la infraestructura de TI:

- La capacidad de crear *instantáneas*, que se registran automáticamente cada vez que se realiza un cambio en el valor de un atributo de un CI. Por ejemplo, cuando se modifica el tamaño de la memoria de un equipo, se genera una instantánea. Esta instantánea registra el estado completo del CI de hardware. El control de versiones puede visualizar la instantánea, indicar los atributos de elemento de configuración que han cambiado y compararla con todas las otras instantáneas históricas del elemento de configuración. Esta información es fundamental cuando se intenta comprender el impacto de los cambios sobre la disponibilidad y el rendimiento de un CI.
- La capacidad de crear *hitos*. Los hitos son instantáneas para fines especiales que se registran con una etiqueta definida por el usuario como, por ejemplo, **Primer día de producción** o **Línea de base de enero**. Dichas etiquetas pueden hacer que se localicen más rápidamente las instantáneas.
- La capacidad de comparar un CI con otro CI que actúa como un estándar. Aunque se puede usar cualquier CI como elemento de configuración estándar para fines de comparación, se recomienda destinar CI específicos para que actúen como *CI estándar*. Un CI estándar permite definir una configuración estándar con la que se pueden comparar los otros CI operativos de la misma familia. Por ejemplo, una organización puede decidir definir **Servidor grande** como elemento de configuración estándar para definir los valores de atributo que definen este tipo de servidor. Se puede hacer que el CI estándar de una familia sea un atributo de un CI operativo de la familia. De esta forma, se podrá comparar el estado actual o cualquier estado histórico de un CI con su configuración estándar asociada. Al igual que en otras comparaciones, puede imprimir esta información o exportarla como archivo delimitado por comas.

Mientras que los hitos pueden actuar como líneas de base no compartidas ni modificables, los elementos de configuración estándar proporcionan líneas de base compartidas y dinámicas para los elementos de configuración.

Importante: un CI estándar nunca debe contener valores para ningún atributo que se utilice para la reconciliación de CI.

El control de versiones incluye las siguientes funciones:

- Captura automática de todas las modificaciones de elementos de configuración.
- Instantáneas de un CI en cualquier momento a partir de cambios de fechas o atributos.
- Varios niveles de visualización, incluidas las vistas detalladas Registro, Básica y Avanzada.
- Comparaciones de múltiples atributos con otras instantáneas, hitos definidos por el usuario o CI estándar.
- Instantáneas automáticas cada vez que los tickets de cambio de CA Service Desk Manager cambian de estado.
- Filtrado y comparación avanzados con soporte de impresión y exportación a CSV.

Más información:

[Usos del control de versiones](#) (en la página 521)

[Registros de activos compartidos y de seguimiento de auditoría de CI](#) (en la página 522)

[Terminología del control de versiones](#) (en la página 523)

[Orígenes de datos del control de versiones](#) (en la página 526)

[Change Management Integration de CA SDM](#) (en la página 527)

[Integración de CA APM](#) (en la página 528)

[Gestión de control de versiones de CI](#) (en la página 529)

[Gestión de cambios de CA SDM](#) (en la página 547)

Usos del control de versiones

El control de versiones incluye los usos siguientes:

- Determinación de problemas

Para corregir un problema con un CI, necesita entender qué cambió en el entorno de ese CI. El control de versiones muestra su estado incorrecto actual, así como su estado en cualquier momento pasado. Esto permite comparar los dos estados para ayudarlo a identificar posibles problemas.

- Planificación de capacidad y rendimiento

La consulta del historial de un CI permite a los encargados de planificar el rendimiento o la capacidad determinar con más precisión las causas de los cuellos de botella del rendimiento y planificar el futuro crecimiento del sistema.

- Conformidad

Puede comparar el estado de un CI con el CI estándar de su familia en cualquier momento de su ciclo de vida de gestión de cambios y garantizar así que el CI está en conformidad y ayudar a identificar los atributos que deban corregirse.

Registros de activos compartidos y de seguimiento de auditoría de CI

La función Control de versiones incluye los cambios de seguimiento de auditoría realizados a CA APM. La función Control de versiones también admite el inicio en contexto desde CA CMDB a CA APM directamente desde cualquier entrada de registro del atributo que está asociado con cada cambio de CA APM. La información de seguimiento de auditoría de CA APM sólo está disponible para CI/activos de las familias de CA CMDB con la función de registro de auditoría de CA APM habilitada.

La ficha Control de versiones que incluye la información de seguimiento de auditoría de CA APM sólo está disponible para CI/activos de las familias de CA CMDB, los activos que no pertenecen a las familias de CA CMDB no se muestran.

De forma predeterminada, CA APM no registra los cambios de atributos de activos. Para utilizar el control de versiones de CA CMDB con un CI/activo gestionado por CA APM, la opción Almacenar datos de pista de auditoría debe estar activada en cada atributo de activo que requiere registro.

Nota: Para obtener más información acerca de cómo activar la auditoría, consulte la documentación de CA APM.

Cuando los atributos de activo se modifican en CA APM, los datos de la ficha Control de versiones de la página Detalles de CI se pueden actualizar antes que los datos de la ficha Atributos; esto se debe a la actividad de almacenamiento en memoria caché. Para volver a sincronizar los valores, haga clic en el botón Editar.

Terminología del control de versiones

El control de versiones es la práctica de representar y seguir *transiciones de servicio*. El control de versiones utiliza habitualmente una convención de nomenclatura para identificar las fechas, las secuencias y los significados de dichas transiciones. Estos registros se pueden utilizar para identificar y comparar estados específicos de un elemento de configuración (CI).

Ejemplo: comparación de versiones

En el caso de un elemento de configuración de aplicación de nóminas, una comparación de la versión 3 con la versión 2 indica las funciones mejoradas y otras diferencias de la versión más reciente.

Más información:

[Estados](#) (en la página 523)

[Versiones](#) (en la página 523)

[Instantáneas](#) (en la página 523)

[Categorías](#) (en la página 524)

[Hitos](#) (en la página 524)

[Elementos de configuración estándar](#) (en la página 525)

Estados

En el contexto del control de versiones, el *estado* de un CI representa todos los valores de atributo de dicho CI en un momento dado. El estado de un CI puede ser el resultado de cambios de atributos de varios MDR.

Versiones

Una *versión* es una instancia identificada de un elemento de configuración (CI) dentro de una PBS (estructura de desglose del producto) o estructura de configuración. Las versiones se utilizan para seguir y auditar el historial de cambios.

Instantáneas

Una *instantánea* es una representación del estado íntegro de un CI en un momento dado. Un CI típico tiene muchas instantáneas asociadas. Una instantánea consolida todos los eventos de modificación que se producen en un CI en un intervalo de un minuto. Por ejemplo, si un CI se actualiza (se edita y se guarda) varias veces en un minuto, se crea una única instantánea que captura todas las actualizaciones durante ese minuto.

Instantánea es un término general que se refiere a instantáneas basadas en hora y fecha, así como hitos o CI estándar. Para ayudarle a localizar momentos especialmente significativos, CA CMDB permite etiquetar las instantáneas de una manera que tenga significado. Estas instantáneas con nombre se denominan hitos.

Todas las veces que se le realice un cambio a un CI, se crea una instantánea automáticamente, sin necesidad de ninguna acción manual. El control de versiones captura todos los cambios del CI, si se han creado mediante la interfaz de usuario o se han originado en un MDR y han llegado a la CMDB a través de GRLoader o los servicios Web de CA CMDB.

Categorías

Una *categoría* identifica una clase de atributos. Habitualmente, la categoría es el nombre de la ficha que muestra los atributos.

Nota: A los elementos que no se encuentran en una ficha (por ejemplo, el nombre, el número de serie y el indicador activo) se les asigna una categoría que no es el nombre de una ficha.

Ejemplos: fichas y categorías

En los siguientes ejemplos se muestra cómo las categorías corresponden a fichas:

- Debido a que *espacio en disco* aparece en la ficha Atributos, su categoría es *Atributos*.
- Debido a que *dirección IP* aparece en la ficha Inventario, su categoría es *Inventario*.
- *Hito* aparece en la categoría *General*.
- El *Elemento de configuración estándar* aparece en la categoría Clasificación.
- *Relaciones* aparece en la categoría Relación.

Hitos

Un *hito* es una instantánea de un CI etiquetada a petición que se crea para marcar un evento, un punto de ruptura lógico o una acumulación de cambios. Contiene el estado real del CI en el momento en el que se fue creada la instantánea. Los hitos permiten identificar rápidamente y desplazarse a puntos significativos en el historial de un CI. Cuando se crea un hito, se crea también una instantánea de "fecha" equivalente.

Los hitos son específicos del elemento de configuración, no se comparten. Al crear un hito para un objeto de alto nivel (por ejemplo, un servicio), los componentes secundarios de dicho objeto de alto nivel no crean hitos automáticamente. Para realizar un hito para un objeto que esté formado por varios componentes secundarios, puede ser útil generar varios hitos independientes.

Los hitos son estáticos y nunca se pueden cambiar ni suprimir. Cuando crea un hito, la instantánea corresponde al estado actual del CI. Luego, cuando se muestran o se utilizan en una comparación, siempre hacen referencia a momentos dados del pasado. Una buena convención de denominación para sus hitos le ayuda a fácilmente identificar puntos críticos en la vida de un CI.

Elementos de configuración estándar

Un *CI estándar* es una configuración abstracta de una familia de CI que se puede utilizar para realizar comparaciones de línea de base con instancias de CI "reales" de la misma familia. Un CI estándar puede ser un CI real en el sentido de que representa un objeto físico o puede existir solamente con fines de comparación. Los CI estándar pueden tener las siguientes asociaciones:

- Un CI estándar se puede compartir entre varios CI.
- Un CI solamente puede tener un único CI estándar asociado a él en un momento dado. Cuando se cambia el CI estándar, dicho cambio se refleja en las comparaciones entre cualquiera de los CI asociados y el CI estándar.
- Una familia puede tener varios CI estándar. Por ejemplo, una familia podría tener elementos de configuración estándar denominados "Servidor de prueba estándar", "Servidor de producción estándar", "Servidor de aceptación estándar". Es recomendable asignar a los elementos de configuración estándar un nombre mediante el cual se puedan buscar e identificar fácilmente como elementos de configuración estándar.

Debido a que el elemento de configuración estándar es un CI en sí mismo, se puede gestionar. Tiene un seguimiento de auditoría, seguridad, un historial de cambios, etc. de igual forma que cualquier otro CI. Una vez que se ha definido un CI estándar para un determinado CI, se puede utilizar para verificar la conformidad con los estándares corporativos.

El concepto de "fecha" u "hora" no se aplica cuando se compara un CI estándar con una instantánea o con un hito. Para fines de comparación sólo se utilizan los valores de atributos del CI estándar. Las instantáneas y los hitos específicos del CI estándar no son aplicables.

Ejemplo: uso del elemento de configuración estándar

Una compañía define una configuración **Estación de trabajo de empleado** como un CI estándar para compararlo con sus equipos de escritorio reales en la familia Hardware.Workstation. Dicha comparación muestra que un determinado equipo sólo tiene 1 GB de RAM, en lugar del valor de memoria del CI estándar de 2 GB.

Orígenes de datos del control de versiones

Los datos del control de versiones se generan siempre que se crea o se modifica un CI mediante cualquier componente que sea compatible con la utilidad de registro de auditoría. Las instantáneas creadas a partir de varias fuentes no se pueden distinguir entre sí. Cuando el entorno está correctamente configurado, las instantáneas aparecen automáticamente siempre que se realicen cambios en los CI y sus relaciones.

Todas las familias de CA CMDB son compatibles con el control de versiones. Los CI de las familias base de CA Service Desk se deben convertir en familias de CA CMDB para aprovechar las funciones del control de versiones.

Los datos del control de versiones incluyen las fuentes:

- **Actualizaciones de CI de CA CMDB:** actualizaciones de atributos comunes del CI y atributos específicos de la familia del CI mediante la interfaz de usuario.
- **Actualizaciones de relaciones de CA CMDB:** actualizaciones de relaciones de la ficha Relaciones y de la lista de relaciones de CI mediante la función Editar y Editar en lista.
- **GRLoader:** actualizaciones de atributos e inserciones de CI, actualizaciones de relaciones, asignaciones de CI estándar e hitos importados mediante GRLoader. Cuando las actualizaciones de un MDR se envían mediante GRLoader, también se registra la fuente del MDR. Esto permite hacer un seguimiento de los cambios en los atributos directamente hasta su fuente.

Nota: Para obtener más información, consulte la *Guía de referencia técnica*.

- **Historial de cambios de CA Service Desk Manager:** se crea automáticamente una instantánea para todos los CI asociados con un ticket de cambio. Se toman hasta cuatro instantáneas cuando el elemento de configuración se abre, se cierra, se activa o se resuelve.

- **Cambios de CI de CA Asset Portfolio Management (CA APM):**
cambios hechos por CA APM a CI con registro habilitado.

Nota: Los CI creados en CA Service Desk o en versiones anteriores de CA CMDB solamente contienen cambios modificatorios. Los valores de atributo iniciales como, por ejemplo, el nombre, la familia y la clase no fueron registrados y no aparecen en las instantáneas. Además, las relaciones creadas con CA Service Desk o con versiones anteriores de CA CMDB no tienen información del historial de auditoría.

Change Management Integration de CA SDM

Los datos del control de versiones se generan para cada CI asociado con un ticket de cambio de CA Service Desk Manager. Cuando el ticket de cambio se mueve de abierto a activo a resuelto a cerrado, se realiza una instantánea de cada CI asociado. De esta forma, se crean instantáneas para los estados abierto, cerrado, activo o resuelto. Si no hay ningún CI asociado con una petición de cambio, no se toman instantáneas.

Nota: La función de control de versiones no requiere ninguna configuración especial y se admite automáticamente en las instalaciones integradas.

La función de control de versiones trata al ticket de cambio de la siguiente manera:

1. Compara el estado del CI en el momento en que el ticket se abrió con su estado actual.
2. Verifica que todos los cambios necesarios se hayan ejecutado correctamente y que no se haya introducido ningún cambio adicional.
3. Cierra el ticket después de que los cambios se hayan validado.

Para fines de auditoría, se puede comparar fácilmente el estado del CI antes y después de realizar cada cambio. Esta información se utiliza para responder a preguntas que incluyan el estado de un CI antes y después de una petición de cambio, por ejemplo:

- ¿Se ha producido el cambio apropiado tal como se solicitaba?
- ¿Qué otros cambios se han producido en el CI que no se relacionen con el ticket de cambio?
- ¿A qué hora se produjeron los cambios?
- ¿Cómo se compara este CI con la configuración estándar, tanto antes como después del cambio?

Integración de CA APM

El control de versiones muestra cambios hechos por CA APM a sus CI. El control de versiones también admite el inicio en contexto de CA CMDB a CA APM directamente desde cualquier entrada del registro de atributo que se haya asociado con un cambio de CA APM. La información de auditoría de CA APM está solamente disponible para los CI de familias de CA CMDB cuando se habilita el registro de auditoría de CA APM.

Nota: Cuando los atributos de CI se modifican en CA APM, los datos de la ficha Control de versiones de la página Detalles de CI se pueden actualizar antes que los datos de la ficha Atributos; esto se debe a la actividad de almacenamiento en memoria caché. Para volver a sincronizar los valores, haga clic en el botón Editar.

De forma predeterminada, CA APM no registra los cambios de atributos de CI. Para utilizar el control de versiones con un CI gestionado por CA APM, la opción Almacenar datos de pista de auditoría debe estar activada en cada atributo de activo que requiere registro.

Nota: De forma predeterminada, hay un retraso de diez minutos desde el momento en que se actualiza un CI en CA APM hasta el momento en el que está disponible para el control de versiones en CMDB. Puede modificar este retraso cambiando la variable @NX_DBMONITOR_TIMER_MINUTES en una instalación integrada.

Nota: Para obtener información sobre cómo habilitar el registro de atributos para los activos, consulte la documentación de CA APM.

Más información:

[Capacidades de integración de CA APM](#) (en la página 528)

Capacidades de integración de CA APM

CA CMDB ofrece las siguientes capacidades de integración con CA APM:

- Los registros compartidos y el registro de auditoría que diferencian entre los CI y los activos de CA APM
- El inicio en contexto de CA CMDB y CA APM para la información del CI/activo
- Los campos de la tabla de extensión compartida
- Actualizaciones de contacto de CA Service Desk Manager cuando CA APM cambia un contacto esencial
- Modificación del tipo de activo de CA APM para utilizar familias de CI

Gestión de control de versiones de CI

Puede mostrar y gestionar el historial del CI, los hitos, las instantáneas asociadas y otras vistas utilizando la ficha Control de versiones. Utilice el panel de la izquierda para navegar y el panel de la derecha para mostrar detalles del CI detalles y el registro de auditoría. Cuando selecciona una instantánea o hito en el panel de la izquierda, el panel de la derecha muestra los valores de atributo de la comparación, el evento o el estado de ese CI. El panel de la izquierda puede mostrar hitos e instantáneas de CI por fecha y hora (modo básico) o por características de CI (modo avanzado), e incluye los siguientes vínculos para ayudarle a gestionar un CI:

Crear hito

Etiqueta el estado de un CI.

Mostrar registro

Muestra el historial de CI no filtrado.

Avanzada/básico

Alterna entre las vistas de instantáneas.

Ocultar valores vacíos

Permite filtrar los campos de datos vacíos. Si no se selecciona, se muestran todos los atributos del CI.

Imprimir y exportar

Imprima o corte y pegue para guardar los datos del control de versiones que se muestran.

Mostrar sólo datos recientes

Cuando un CI tiene muchas instantáneas o relaciones, puede seleccionar solamente los datos del control de versiones más recientes para reducir el tiempo necesario para que se muestre. El mensaje "¿Desea cargar los datos recientes solamente?" indica el límite de muestra. Puede actuar de la siguiente manera:

- Haga clic en Cancelar para mostrar todos los datos.
- Haga clic en Aceptar para mostrar solamente las instantáneas más recientes tanto en la vista básica como en la vista avanzada.

Nota: El historial que muestra los MDR, quién realizó la última modificación y el ID de usuario no se muestra para las instantáneas que se omitieron. Las instantáneas para fechas antes de la instalación de CA CMDB r12.5 pueden no incluir los MDR ni la información de quién realizó la última modificación.

Mostrar registro

El registro permite ver el historial de un elemento de configuración. La opción Filtrar permite filtrar las filas del registro. Imprimir y exportar permite imprimir o copiar y pegar para guardar los datos del control de versiones en pantalla.

El panel de información de Configurando la versión muestra los siguientes campos:

- Categoría
- Date
- Registro
- Atributo
- Valor nuevo
- Valor anterior
- Modificado por
- MDR

Nota: El registro sólo muestra *actualizaciones* de atributos para los CI creados en versiones anteriores de CA Service Desk Manager o CA CMDB. No muestra los valores de atributo iniciales del CI. Las relaciones creadas en versiones anteriores de CA Service Desk Manager o CA CMDB no incluyen la información del historial de auditoría y no aparecen en el registro.

Filtrado de registros

El registro se puede filtrar introduciendo una cadena sencilla en el campo Filtro. El filtro no distingue entre mayúsculas y minúsculas. Si la cadena de filtrado aparece en cualquier lugar de una fila del registro, se mostrará dicha fila. En el filtro no se utilizan caracteres especiales ni caracteres comodín. Se mostrarán las filas del registro que coincidan con los criterios de filtrado, y las que no coincidan se ocultarán.

No necesita pulsar Intro ni actualizar para actualizar la pantalla. La vista del registro se filtra al pulsar cada tecla y se aplica a todos los campos: Fecha, Registro, Atributo, Valor antiguo, Valor nuevo, MDR y Nombre.

Visualización del historial de elementos de configuración

Se puede ver el historial de un elemento de configuración.

Para ver el historial de elementos de configuración

1. Busque y abra el elemento de configuración.
Aparecerá la página de detalles del elemento de configuración.
2. Haga clic en la ficha Configurando la versión.
Aparece la página Control de versiones.
3. Haga clic en Mostrar registro.
Se listará el historial de elementos de configuración.

Nota: Mostrar registro ignora las selecciones del panel izquierdo.

Impresión del registro de un CI

Puede imprimir el registro de un CI.

Para imprimir el registro de un CI

1. Seleccione el CI y haga clic en la ficha Configurando la versión.
2. Haga clic en el vínculo Mostrar registro.
3. (Opcional) Introduzca los criterios de filtrado deseados para ocultar/mostrar las filas del registro.
4. Haga clic en Imprimir.
Se abrirá una ventana apta para la impresión. Se mostrará el informe del control de versiones para el CI.
5. Para imprimir una copia del informe, utilice la ventana del explorador Web para hacer clic en Archivo, Imprimir.
El texto con formato se envía a la impresora definida.

Compatibilidad con exportación a CSV

Puede exportar el contenido del registro de CA CMDB a un archivo con formato de valores separados por comas (CSV) que pueden importar las aplicaciones o herramientas de informe de terceros. La exportación se basa en la visualización actual, que puede estar filtrada o sin filtrar.

Más información:

[Exportación de datos de elementos de configuración](#) (en la página 543)

CA SDM integrada y registros de CA APM

Además de los cambios que se realizaron mediante las utilidades de CA CMDB, el registro del CI también incluye eventos de actualización de actividades de tickets de cambio de CA Service Desk Manager y actualizaciones de CA APM.

Más información:

[Integración de CA APM](#) (en la página 528)

Identificación de la fuente e inicio en contexto del MDR

CA CMDB proporciona una forma de iniciar en contexto, directamente desde el registro al proveedor de datos del MDR para una entrada de registro del CI concreta. Esta función de inicio hace lo siguiente:

- Hace un seguimiento de los cambios de los atributos hasta el MDR de origen, cuando el MDR ha usado las etiquetas <mdr_name> <mdr_class> y <federated_asset_id> en la entrada de GRLoader.

Nota: Para obtener más información, consulte la *Guía de referencia técnica de CA CMDB*.

- Identifica si un atributo de un CI está siendo actualizado por más de un MDR. Esta situación se produce cuando varios MDR proporcionan datos independientemente a una definición del CI.
- Identifica qué MDR está actuando como la fuente autorizada.

Nota: Las entradas de registro creadas en CA Service Desk o en versiones anteriores de CA CMDB no contienen información del inicio en contexto del MDR. Además, CA Cohesion ACM proporciona información de inicio del MDR para la mayoría, pero no todos, los atributos o relaciones.

Nombres de atributo

Los nombres de atributos mostrados en el registro coinciden con el nombre de atributo mostrado en la interfaz de usuario. Ya no reflejan el nombre de objeto interno. Por ejemplo, CA CMDB muestra "Tipo de Mantenimiento" en lugar de "mtce_type".

Registro de familias y atributos personalizados

Para habilitar el registro de familias y atributos personalizados, especifique los atributos nuevos de MDR y desencadenantes de auditoría. Si crea familias o atributos nuevos, también debe crear los archivos de metadatos correspondientes para especificar los nombres de atributo legibles que se mostrarán en el registro; de otro modo, aparecerá el nombre de objeto interno.

Nota: Para obtener más información, consulte la sección Ampliación de CA CMDB en la *Guía de administración*.

Creación de un hito

Puede crear un hito en la interfaz de usuario o utilizando GRLoader.

Para crear un hito desde la interfaz de usuario

1. Seleccione el CI y haga clic en la ficha Configurando la versión.
2. Haga clic en Crear hito.
3. Introduzca un texto descriptivo para el hito. Haga clic en Guardar.
Se cerrará la página Crear hito.
4. Seleccione Ver, Actualizar.

La vista básica muestra una nueva instantánea, con la fecha y la hora actuales, que representa el hito que acaba de crear. Si se cambia a la vista Hito, se mostrarán sólo las instantáneas con nombres asignados. Los hitos se muestran en secuencia de fecha/hora descendente, con el más reciente en la parte superior.

Para crear un hito mediante GRLoader

1. Agregue la etiqueta <milestone> al XML para ese CI.
2. Aplique las mismas reglas de reconciliación que se utilizan al asociar un hito con un CI.

Nota: El valor de la etiqueta del hito es la etiqueta asociada con dicho hito.

3. Guarde y cierre el XML para el CI.
Se crea el hito.

Nota: Para obtener más información, consulte la *Guía de referencia técnica de CA CMDB*.

Ejemplo: uso de GRLoader para crear un hito

La siguiente muestra de GRLoader crea el hito **Fin del año fiscal 2008**.

```
<ci>
<name>servidor1 </name>
<milestone>Fin del año fiscal 2008</milestone>
</ci>
```

Creación de un elemento de configuración estándar

Un elemento de configuración estándar se crea de igual forma que cualquier otro elemento de configuración.

Para crear un elemento de configuración estándar en la interfaz de usuario

1. Seleccione Crear nuevo elemento de configuración en el menú Archivo.
2. Seleccione la familia que quiere utilizar para el nuevo CI estándar.
3. Defina los atributos, al igual que con cualquier CI normal.
Se crea el CI estándar.

Nota: Cualquier elemento de configuración puede actuar como un elemento de configuración estándar, pero se aplican las siguientes precauciones:

- Un elemento de configuración estándar debe seguir una convención de nomenclatura para no confundirlo con los elementos de configuración normales.
- Un elemento de configuración estándar sólo debe actuar como línea de base para los CI de la misma familia que el CI estándar.
- A un CI estándar *no* se le debe asignar valores para ningún atributo usado en la reconciliación, por ejemplo, la dirección MAC, el número de serie, el ID elem. config. alter., el DNS, etc).
- Como los elementos de configuración estándar no se distinguen de los CI normales, aparecen en el panel de resultados y se cuentan en el número total de CI.
- Es mejor que un elemento de configuración estándar no represente ninguna instancia real de un objeto de empresa.

Asignación de un elemento de configuración estándar a un elemento de configuración

Puede asignar un elemento de configuración estándar a un elemento de configuración utilizando la página Detalles de CI. Puede asignar un CI estándar a una lista de CI o utilizando la opción Editar en lista.

Para asignar el elemento de configuración estándar estándar de una familia a un CI mediante la página de detalles del CI

1. Seleccione un CI y haga clic en Editar.
Aparecerá la página Actualización del elemento de configuración.
2. Haga clic en el icono situado junto al campo Elem. de config. estándar.
Se mostrará la lista de elementos de configuración.
3. Seleccione un CI que actúe como el elemento de configuración estándar.
Haga clic en Guardar.
Se asigna el elemento de configuración estándar.

Para asignar elementos de configuración estándar a una lista de elementos de configuración mediante Editar en lista

1. En el panel de resultados o la ficha Administración especifique el filtro de búsqueda para mostrar un único CI o varios CI en la lista de detalles y haga clic en Buscar.
Aparecerá una lista de todos los CI que coincidan con los criterios de búsqueda.
2. Haga clic en el botón Editar en lista en la parte superior derecha de la lista de resultados.
Se mostrarán los controles de Editar en lista del CI.
3. Seleccione la fila que contiene el CI para asignar también el elemento de configuración estándar.
La fila se muestra en un color resaltado.
4. Haga clic en el icono situado junto al campo Elem. de config. estándar.
Se mostrará la lista de elementos de configuración.
5. Seleccione un CI que actúe como el elemento de configuración estándar.
Haga clic en Guardar para actualizar el CI único o en Cambiar todo para actualizar todos los elementos de configuración de la lista.
El elemento de configuración estándar se asigna al CI único (Guardar) o a todos los elementos de configuración de la lista (Cambiar todo).

Nota: Cualquier elemento de configuración puede actuar como un elemento de configuración estándar, pero se aplican las siguientes precauciones:

- Un elemento de configuración estándar debe seguir una convención de nomenclatura para no confundirlo con los elementos de configuración normales.
- Un elemento de configuración estándar sólo debe actuar como línea de base para los CI de la misma familia que el CI estándar.
- A un CI estándar *no* se le debe asignar valores para ningún atributo usado en la reconciliación, por ejemplo, la dirección MAC, el número de serie, el ID elem. config. alter., el DNS, etc).
- Como los elementos de configuración estándar no se distinguen de los CI normales, aparecen en el panel de resultados y se cuentan en el número total de CI.

Es mejor que un elemento de configuración estándar no represente ninguna instancia real de un objeto de empresa.

Asignación de un elemento de configuración estándar a un elemento de configuración mediante GRLoader

Para asignar un CI estándar a un CI, incluya la etiqueta <standard_ci> en la descripción del CI.

Nota: Para obtener más información, consulte la *Guía de referencia técnica de CA CMDB*.

Ejemplo: asignación de un CI estándar a un CI

Si tiene la configuración de una estación de trabajo estándar almacenada en un CI denominado **configuración de estación de trabajo estándar**, puede asignar dicho CI estándar a la estación de trabajo de Juan. Para hacerlo, utilice GRLoader para cargar el siguiente XML:

```
<ci>
  <name>Estación de trabajo de Juan</name>
  <class>Server</class>
  <standard_ci>configuración de estación de trabajo estándar</standard_ci>
</ci>
```


Uso de la vista básica

Las instantáneas se pueden seleccionar en la vista básica o avanzada. En ambos modos se pueden mostrar los mismos tipos de datos de control de versiones. La vista básica le permite ver fácilmente el estado de un CI.

Para utilizar la vista básica para ver el estado de un CI

1. Abra el elemento de configuración en la interfaz de usuario y haga clic en la ficha Control de versiones.

Las instantáneas existentes se muestran en la parte izquierda de la página.

2. Seleccione un tipo de instantánea en la lista desplegable de tipos de instantáneas:

Nota: Si se especifica un CI estándar para el CI central, se muestra en la parte superior de la lista de instantáneas o hitos, y se indica mediante el indicador "Elem. de config. estándar" a la derecha del nombre del CI. Si hace clic en un CI estándar, aparecen los atributos para él y no el CI central.

Instantánea

Lista todas las instantáneas del CI identificadas basado en la fecha/hora y el CI estándar. Ésta es la opción predeterminada.

Hito

Lista todos los hitos definidos por el usuario y el CI estándar.

El estado del CI se muestra en el panel derecho.

El área de texto informativo de la parte inferior muestra información sobre el elemento actual sobre el que está colocado el puntero del ratón. Al colocarse sobre una instantánea, un hito o un CI estándar se muestra información sobre la fecha y la hora en que se creó y el tipo de instantánea.

Nota: Puede seleccionar dos o más instantáneas, hitos, o CI estándar para compararlos.

Uso de la vista avanzada

Las instantáneas se pueden seleccionar en la vista básica o avanzada. En ambos modos se pueden mostrar los mismos tipos de datos de control de versiones. La vista avanzada le permite ver instantáneas basado en el tipo de atributo, valor e indicación de tiempo. Esta vista también permite realizar comparaciones "de cualquiera con cualquiera" con atributos, hitos o un CI estándar. Una jerarquía de árbol muestra una carpeta para cada atributo del CI, y cada carpeta de atributo contiene un historial de los valores del atributo. La jerarquía se organiza del siguiente modo:

Raíz

- Nombre de atributo
 - valor de atributo 1
 - valor de atributo 2

Esta jerarquía le permite echar un vistazo del historial de valores exclusivos para cualquier atributo particular.

Para utilizar la vista avanzada

1. Abra el elemento de configuración en la interfaz de usuario y haga clic en la ficha Control de versiones.

Las instantáneas existentes se muestran en la parte izquierda de la página.

2. Haga clic en Avanzadas.

Selección avanzada muestra una jerarquía de carpetas.

3. Desplácese por la jerarquía de carpetas y haga clic en la carpeta que incluye la información que quiere ver:

Date

Lista las instantáneas basada en la fecha/hora, que son idénticas a la vista básica. Las instantáneas se pueden subdividir aún más basándose en el año/mes si hay 30 o más instantáneas para el CI. El elemento de configuración estándar también se lista en esta carpeta si se ha asignado uno al CI central.

Hito

Lista todos los hitos definidos por el usuario, que son idénticos a la vista básica. El elemento de configuración estándar también se lista en esta carpeta si se ha asignado uno al CI central.

Los atributos del elemento de configuración estándar se muestran como nodos de hoja del árbol especiales con un "elemento de configuración estándar". Los valores del elemento de configuración estándar sólo aparecen para atributos para los cuales hay un valor de elemento de configuración estándar. No aparecen para atributos en los que no se ha establecido el valor.

Relación

Contiene todas las relaciones (pasadas y actuales) para el CI. La jerarquía de carpetas transmite la siguiente información:

Relación

Tipo de relación

CI asociado

Estado y fecha

Tipo de relación especifica la clase de relación, como por ejemplo "está contenido en", "alberga" o "comunica con".

CI asociado es el nombre del CI asociado con la relación.

Estado y fecha especifica el estado de la relación en la fecha y hora especificada. Los valores de estado incluyen los siguientes:

- Relación creada: estado del CI cuando se creó la relación.
- Relación finalizada: este CI ya no participa en la relación. La relación continúa existiendo en el extremo asociado de la relación, pero el CI central no está implicado.
- Relación suprimida: la relación se marcó como suprimida.
- Relación modificada: la relación se reactivó desde el estado suprimido.
- Nuevo partner y tipo: el extremo de partner de la relación ha sido asignado a un nuevo CI y, al mismo tiempo, se cambió el tipo de relación.
- Nuevo tipo de relación: el tipo de relación entre dos CI ha cambiado.
- CI de partner asignado: el extremo de partner de la relación ha cambiado.

4. Haga clic en un valor de atributo.

Se muestra el estado total del CI en el momento en que el valor de atributo se estableció.

Ejemplo: uso de la vista avanzada para mostrar los atributos de espacio en disco

En el siguiente ejemplo, Selección avanzada muestra el espacio en disco aumentado de entre 10 y 20 a 100 GB.

Raíz

Espacio en disco
10 GB
20 GB
100 GB

Haga clic en cualquier valor para ver cuándo se produjo el cambio, el estado de los otros atributos cuando se produjo el cambio y el número de la petición de cambio que se abrió cuando se cambió el espacio en disco.

Visualización de los detalles de la instantánea

Puede ver detalles de la instantánea en la vista avanzada o básica.

Para ver los detalles de la instantánea

1. Abra el elemento de configuración en la interfaz de usuario y haga clic en la ficha Control de versiones.

Aparecerá una lista de las instantáneas existentes en el lado izquierdo de la página.

2. Haga clic en una instantánea.

Se muestran los detalles en el panel derecho de las vistas básica y avanzada. Cuando solamente se selecciona un único elemento, el panel derecho muestra información sobre el estándar, el hito o la instantánea seleccionada.

Los datos mostrados incluyen los siguientes detalles e indicadores:

Ocultar valores vacíos

Permite filtrar los campos de datos vacíos. Si no se selecciona, se muestran todos los atributos del CI.

Texto del campo del valor en negrita

Indica que un atributo o relación ha cambiado desde que se tomó la última instantánea. Al ver los detalles de un elemento de configuración estándar, todos los valores están en negrita.

Valor

Muestra el valor anterior del atributo y la hora del último cambio cuando se coloca el puntero sobre el valor. La información aparece en un área de texto en la parte inferior de la ficha Control de versiones.

valor “(en blanco)”

Indica si se borró un valor anterior.

Categoría de relación

Muestra información sobre la relación, incluso información sobre el CI del partner y el tipo.

Inicio en contexto de MDR e identificación de la fuente

Proporciona inicio en contexto a un MDR de proveedor desde la entrada de detalles del elemento de configuración.

Nota: Los CI creados en CA Service Desk o en versiones anteriores de CA CMDB podrían no tener la información de MDR ni de quién ha realizado la modificación. Además, CA Cohesion ACM proporciona inicio en contexto de MDR para la mayoría pero no todos los atributos o relaciones.

Realiza un seguimiento de los cambios de atributos hasta el MDR de origen.

Detecta cuándo un atributo del CI está siendo actualizado por más de un MDR. Esta situación se produce cuando varios MDR proporcionan datos independientemente a una definición del CI.

Identifica el MDR que actúa como la fuente autoritativa.

Visualización del estado de un CI en una fecha específica (vista básica)

Puede utilizar la vista básica para ver el estado de un CI en una fecha específica.

Para ver el estado de un CI en una fecha específica

1. Seleccione un CI y desplácese hasta su página de detalles.
2. Haga clic en la ficha Configurando la versión.

Se mostrará la vista básica del CI.

3. Seleccione la fecha que desee.

El lado derecho de la pantalla muestra el estado del CI en la fecha seleccionada.

Visualización del estado de un CI en una fecha específica (vista avanzada)

Puede utilizar Selección avanzada para ver el estado de un CI en una fecha específica.

Para ver el estado de un CI en una fecha específica

1. Seleccione un CI y desplácese hasta su página de detalles.
2. Haga clic en la ficha Control de versiones y, a continuación, haga clic en Avanzadas.

Se mostrará el árbol de selección avanzada.

3. Expanda la carpeta Fecha.
4. Seleccione la fecha en la que desea ver el CI.

Se mostrará el estado del CI en dicha fecha.

Inicio del MDR que estableció un atributo

Si el historial para un CI hace referencia a un MDR, puede iniciar un MDR para ver detalles del CI.

Para iniciar un MDR con el fin de ver los detalles del CI

1. Seleccione un CI y desplácese hasta su página de detalles.
2. Haga clic en la ficha Configurando la versión.
3. Haga clic en Mostrar registro o seleccione el hito o la instantánea del CI que quiera ver.
4. Seleccione la fila del atributo que desea investigar.
5. Si el historial del CI hace referencia a un MDR, haga clic en el vínculo del MDR.

El MDR del proveedor muestra detalles adicionales del CI.

Impresión de una instantánea de un CI

Puede imprimir una instantánea de un CI en un fecha seleccionada.

Para imprimir una instantánea de un CI en la fecha seleccionada

1. Seleccione el CI y haga clic en la ficha Configurando la versión.
2. Seleccione la vista básica.
3. Seleccione Instantánea en la lista desplegable Tipo de instantánea.
4. Seleccione una fecha en la lista de fechas de la izquierda.

5. Haga clic en Imprimir.
Aparece una ventana apta para la impresión y muestra el informe de control de versiones para el CI.
6. Para imprimir el informe, utilice la ventana del explorador Web y haga clic en Archivo, Imprimir.
El texto con formato se envía a la impresora definida.

Impresión de un hito de un CI

Puede imprimir un hito de un CI en una fecha seleccionada.

Para imprimir un hito de un CI en la fecha seleccionada

1. Seleccione el CI y haga clic en la ficha Configurando la versión.
2. Seleccione el hito deseado en la vista básica o en la vista avanzada.
3. Haga clic en Imprimir.
Aparece una ventana apta para la impresión y muestra el informe de control de versiones para el CI.
4. Para imprimir el informe, utilice la ventana del explorador Web y haga clic en Archivo, Imprimir.
El texto con formato se envía a la impresora definida.

Exportación de datos de elementos de configuración

La página de exportación del control de versiones a CSV le permite exportar la instantánea de CI y la información de registro en un formato de valores separados por comas (CSV). Los datos se muestran en una página de exportación. Los datos con formato corresponden a la vista que obtuvo y las filas aparecen en líneas independientes con los valores separados por comas en columnas incluidos entre comillas dobles. El filtrado y la comparación de datos que se seleccionó en la ficha Control de versiones corresponde a aquello a lo que se le ha aplicado formato para la exportación.

Para exportar datos de CI

1. Seleccione el CI y haga clic en la ficha Configurando la versión.
2. Haga clic en la vista deseada del CI como, por ejemplo: Mostrar registro, una comparación de instantáneas, hito, etc.

3. Haga clic en Exportar.

Se mostrará la página de exportación del control de versiones a CSV para la vista del CI.

4. Utilice la acción Seleccionar todo (en el menú contextual o el atajo de teclado).

5. Utilice cortar y pegar para transferir los datos del CI desde la página con formato a un archivo CSV o a una aplicación de terceros. Por ejemplo, se puede exportar a una hoja de cálculo de Excel.

Se exportan los datos de CI.

Instantáneas y cambios de familia de CI

Los cambios de familia pueden afectar a una instantánea de un CI.

Una instantánea incluye los siguientes tipos de atributos diferentes:

- Atributos comunes
- Atributos específicos de la familia

Cuando cambia la familia de un CI, se producen los siguientes cambios en la instantánea:

- Atributos específicos de la familia asociados con el cambio de CI.
- Los detalles de la instantánea reflejan la familia en el momento de la instantánea.

La familia de un CI determina los atributos del CI. Si cambia un atributo *específico de la familia* y luego cambia la familia del CI, el resultado es un CI que ya no posee el atributo *específico de la familia* que se cambió. Si se cambia la familia de un CI, no se produce ningún efecto en sus atributos *comunes*.

Ejemplo: cambio a la familia asociada con un CI

Este ejemplo muestra los efectos de los cambios a la familia del CI cambios sobre una instantánea de un CI.

Hora	Estados/Cambios
0	El CI está en la Familia1.
1	Se cambia el valor de un atributo específico de la Familia1.
2	Se cambian los valores de varios atributos comunes.
3	La familia del CI se cambia de Familia1 a Familia2. Cuando esto ocurre, todos los atributos específicos de la Familia1 dejan de estar disponibles para este CI.

- 4 Se cambia el valor de un atributo específico de la Familia2.
- 5 Se cambian varios atributos comunes.
- 6 La familia del CI se vuelve a cambiar a Familia1. Cuando esto ocurre, los valores de todos los atributos específicos de la Familia2 dejan de estar disponibles para este CI, pero se restauran los valores de los atributos específicos de la Familia1 anteriores.
- 7 Se cambian varios atributos comunes.
- 8 Se cambia un atributo específico de la Familia1.

En el ejemplo anterior, la instantánea realizada en Hora=7 no contiene información desde los cambios realizados a las horas 3 ó 4. Estos cambios representan los cambios realizados en los atributos específicos de la Familia2.

Comparación de instantáneas (vista básica)

Puede comparar dos o más instantáneas, hitos o elementos de configuración estándar.

Para comparar instantáneas, hitos o CI estándar

1. Seleccione un CI y desplácese hasta su página de detalles.
2. Haga clic en la ficha Configurando la versión.
3. Seleccione un hito o una instantánea en la lista desplegable Tipo de instantánea.

Se listan hitos o instantáneas.

4. Seleccione dos o más instantáneas, hitos o CI estándar.

La vista de comparación muestra los siguientes resultados:

- Una columna muestra cómo difieren las instantáneas o los hitos.
- Cada fila muestra los valores de los atributos para las instantáneas seleccionadas.
- Sólo se muestran los atributos con diferencias. La fecha se muestra siempre, salvo si las instantáneas son idénticas.
- Las comparaciones de elementos de configuración estándar no son específicas de la hora, de modo que sus campos de fecha se establecen en **Elem. de config. estándar**.
- Los resultados de la comparación se pueden imprimir o exportar a un archivo CSV.

Comparación de instantáneas (vista avanzada)

Puede comparar dos o más instantáneas, hitos o elementos de configuración estándar.

Para comparar instantáneas, hitos o CI estándar en la vista avanzada

1. Seleccione un CI y desplácese hasta su página de detalles.
2. Haga clic en la ficha Control de versiones y, a continuación, haga clic en Avanzadas.

Selección avanzada muestra el CI.

3. Desplácese por la jerarquía de carpetas hasta el valor que quiere utilizar para la comparación de instantáneas.
4. Seleccione un valor para cada comparación de instantáneas.

Se muestra la comparación para el CI, por ejemplo, una comparación de instantáneas basada en los valores de carpeta seleccionados.

La vista de comparación muestra los siguientes resultados:

- Una columna muestra cómo difieren las instantáneas o los hitos.
- Cada fila muestra los valores de los atributos para las instantáneas seleccionadas.
- Sólo se muestran los atributos con diferencias. La fecha se muestra siempre, salvo si las instantáneas son idénticas.
- Las comparaciones de elementos de configuración estándar no son específicas de la hora, de modo que sus campos de fecha se establecen en **Elem. de config. estándar**.
- Los resultados de la comparación se pueden imprimir o exportar a un archivo CSV.

Nota: En la vista avanzada, dos CI pueden tener una relación sin tener asignado ningún tipo de relación (por ejemplo, CI creados por CA NSM). Dichos nodos de relación se identifican como (vacío).

Gestión de cambios de CA SDM

Los datos del control de versiones se generan automáticamente para cada CI asociado con un ticket de cambio de CA Service Desk. Cuando el ticket de cambio se mueve de abierto a activo a resuelto a cerrado, se realiza una instantánea de cada CI asociado. El control de versiones permite hacer lo siguiente:

- Comparar el estado del CI con su CI estándar en cualquier punto en un ciclo de vida de gestión de cambios.
- Ayudar a asegurar que el CI está en conformidad y ayuda a identificar esos atributos que necesitan resolución.
- Realizar comparaciones entre los estados del CI en cualquier punto del ciclo de vida de la orden de cambio, pero también en cualquier fecha u hora intermedias.
- Ver el progreso en cada etapa del cambio, incluso cualquier hito.

La integración entre CA Service Desk y CA CMDB se ilustra demostrando cómo puede auditar cambios ejecutados durante el ciclo de vida de gestión de servicios de un CI. En este ejemplo, se utiliza una petición de cambio para actualizar los componentes de un servidor de hardware.

Para crear una orden de cambios y asociarla con un CI

1. Cree un ticket de cambio de CA Service Desk haciendo clic en Archivo, Nueva orden de cambio.
2. Introduzca la información de la petición de cambio y un resumen de la orden, por ejemplo: mejorar la unidad de disco duro a 500 GB.
3. Haga clic en la ficha Elementos de configuración y a continuación haga clic en Actualizar elementos de configuración.
4. Especifique los criterios de búsqueda de elementos de configuración (por ejemplo, el nombre del servidor de hardware) y haga clic en Buscar.
5. En el formulario Actualizar elementos de configuración afectados seleccione los CI asociados con el ticket de cambio (por ejemplo, el servidor de hardware del paso 4) y agréguelos a la lista de elementos de configuración afectados. Haga clic en OK.
6. Guarde la solicitud de cambio.

Para realizar los cambios

1. Haga los cambios necesarios para el CI. Por ejemplo, realice la instalación del disco duro en el equipo físico y luego actualice el atributo de capacidad de disco para el CI del servidor de hardware.
2. Cierre la solicitud de cambio.
3. Para asegurarse de que se completó el cambio, visualice el CI, haga clic en la ficha Control de versiones y compare las instantáneas del CI antes y después de realizar el cambio.

Una comparación del estado del CI entre el momento en que se abrió y se cerró la orden de cambio muestra que el tamaño de la unidad de disco duro del servidor de hardware era de 100 GB antes del cambio, 500 GB después de que se completó el cambio, y la fecha y las horas en las que se produjeron los cambios. Asimismo se mostrará el resto de los atributos que se modificaron entre las horas de apertura y cierre.

Visualización de los atributos de un elemento de configuración en otros productos de CA

Puede utilizar la página Visor de activos comunes para ver atributos de un elemento de configuración en otros productos de CA.

Para ver los atributos de un elemento de configuración en otros productos de CA

1. Localice y abra el elemento de configuración.
2. Haga clic en Visor de activos.
Aparece la página Visor de activos comunes.
3. Haga clic en la ficha de recursos de propiedad para localizar información de los atributos de otros productos de CA.
4. Haga clic en Cerrar ventana cuando haya terminado.

Ha visto atributos de elemento de configuración en otros productos de CA.

Uso del Visor de CMDBf

CA Service Desk Manager proporciona el Visor de CMDBf para mostrar los resultados de la federación de elementos de configuración (CI) en los MDR. En una página de detalles de CI (o en el menú contextual del CI en la lista de elementos de configuración), haga clic en Visor de CMDBf para ver los atributos de CI de las CMDB y los MDR federados en paralelo. En la página Vista federada, puede hacer clic en Recuperar para actualizar la información de cualquiera de los MDR federados. Para facilitar la legibilidad, los archivos de metadatos de CA CMDB pueden conciliar los nombres de atributo de MDR con los de CA CMDB.

Nota: Esta opción requiere que los MDR admitan consultas. Puede configurar los puntos finales de CMDBf de MDR para que muestren sus resultados en Vista federada. Si desea obtener más información, consulte la *Guía de implementación*.

Si el elemento de configuración no tiene datos federados, el visor muestra solamente atributos de CA CMDB.

Visualizador CMDB

CA Service Desk Manager permite adaptar los componentes de TI (*elementos de configuración* o CI) a los servicios de negocio. CA CMDB define *relaciones* entre CI, como cuando un grupo de CI trabaja para proporcionar un servicio de negocio. El Visualizador de CMDB permite ver la imagen completa de las relaciones entre CI y proporciona funciones para gestionar las relaciones. Si se trabaja desde un *CI central* (cualquier CI de interés), puede utilizar el visualizador para mostrar hasta nueve niveles de CI relacionados.

CA utiliza un modelo de proveedor/dependiente para definir relaciones entre elementos de configuración. Todos los elementos de configuración que participan en un servicio de negocios son *proveedores* de dicho servicio de negocios (el *dependiente*). De forma similar, los proveedores pueden ser también *dependientes* de otros CI. Puede usarse el visualizador para realizar los siguientes análisis de proveedor/dependiente:

Examinar

Muestra vistas no filtradas de todos los CI.

Análisis de impactos

Comienza con un CI central (proveedor) y busca sus dependientes.

Causa raíz

Comienza con un servicio de negocio (dependiente) y ve todos los CI que son proveedores de dicho servicio.

Elementos de configuración de causa y efecto

Combina un análisis del impacto y la causa raíz en una búsqueda.

Relación de seguimiento

Muestra todas las posibles relaciones en función de niveles. Si selecciona solamente un CI, este filtro muestra la vista Examinar.

Ruta más corta

Muestra la cadena más corta de relaciones en función de niveles.

El Visualizador de CMDB permite realizar las siguientes acciones:

- Visualizar múltiples niveles de CI desde una vista gráfica configurable
- Controlar o cancelar el progreso del procesamiento
- Buscar utilizando criterios flexibles
- Filtrar basado en familias de CI, tipos de relación y otros atributos
- Mostrar relaciones de CI
- Hacer el seguimiento de una relación entre dos CI
- Visualizar una cadena de dependencia
- Invocar a CA CMDB directamente desde el visualizador
- Mostrar atributos y propiedades de CI
- Guardar metadatos de gráfico
- Imprimir el diseño de gráfico
- Buscar un CI concreto en un gráfico visualizado
- Crear un CI (dependiendo del rol)
- Crear nuevas relaciones de CI (dependiendo del rol)
- Utilizar el borrador para almacenar CI clave
- Mostrar el estado de CI
- Ocultar o revelar un CI en el diseño del visualizador
- Seguridad de datos basada en roles
- Iniciar MDR externos
- Obtener ayuda en línea para las opciones del visualizador

Más información:

[Cómo realizar análisis de causa raíz](#) (en la página 551)

[Administración del visualizador](#) (en la página 552)

Cómo realizar análisis de causa raíz

Si utiliza el visualizador con el visor de CMDBf, puede ejecutar un análisis de causa raíz.

Procedimiento para llevar a cabo un análisis de causa raíz

1. En el visualizador, localice un elemento de configuración de servicio en una condición de problema particular (por ejemplo, lento o no disponible).
2. Haga clic con el botón secundario del ratón en el CI y seleccione Crear elem. de config. central.
3. Seleccione un filtro de causa raíz con los criterios siguientes:
 - Tipo de clase: no disponible
 - Relación de proveedor a dependiente: todas las relaciones que se mostrarán para el análisis de causa raíz.

4. Haga clic en Ver.

En el gráfico resultante, todos los elementos de configuración que se relacionan con el elemento de configuración central se muestran tal y como se especifica en los filtros. Todas las rutas entre elementos de configuración incluyen elementos de configuración intermediarios en el nivel predeterminado.

5. Desplácese a los elementos de configuración e inspecciónelos para ver si tienen incidentes, problemas o cambios recientes como candidatos a la causa raíz de la condición del elemento de configuración central.
6. Inicie CA CMDB en el contexto para un elemento de configuración particular.
7. Haga clic en Visor de CMDBf

La vista federada se muestra con la lista de proveedores de MDR para el elemento de configuración.
8. Haga clic en Recuperar para obtener los últimos atributos de MDR.

Se actualizan los atributos de MDR.

Administración del visualizador

La interfaz de administración del Visualizador puede usarse para editar los valores del Visualizador de CMDB. Estas funciones sólo están disponibles para los roles con privilegios de administrador.

La interfaz de administración del visualizador cuenta con las fichas siguientes:

Ficha Configuración del visualizador

Permite definir la información que se muestra del servidor y de los elementos de configuración.

Ficha Estilo de la relación

Define las características gráficas de la relación.

Nota: Esta página se desactiva en un servidor secundario del visualizador.

Ficha Estado de elem. de config.

Define las características gráficas de los elementos de configuración.

Nota: Esta página se desactiva en un servidor secundario del visualizador.

Ficha Filtros

Permite crear, editar y eliminar filtros para análisis de elementos de configuración.

Nota: Esta página se desactiva en un servidor secundario del visualizador.

Ficha Configuración de iconos

Asigna una familia de CI a su respectiva imagen de icono cuando el Visualizador de CMDB se ha actualizado de r11.2 a r12.5.

Nota: Para obtener más información acerca de las definiciones del Visualizador, consulte la Ayuda en línea del Visualizador de CMDB.

Cómo agregar un activo detectado

Puede convertir activos sin propietario en Management Database (MDB) en elementos de configuración con propietario.

Para localizar y agregar un activo detectado

1. Muestre la lista de elementos de configuración.
Si la lista no aparece en el panel derecho, expanda el nodo de elementos de configuración en el árbol de navegación y haga clic en Todos.
2. Haga clic en el botón Activos detectados.
Aparecerá la página Búsqueda de activos detectados.
3. Haga clic en Buscar para mostrar la lista de activos detectados.
4. En la lista, seleccione el activo que desea agregar como un elemento de configuración. A continuación, haga clic con el botón derecho del ratón en el activo y seleccione Crear nuevo elemento de configuración en el menú emergente.
Aparecerá la página Crear nuevo elemento de configuración con información sobre el elemento en algunos de los campos.
5. Complete el resto de campos que aplican al nuevo elemento de configuración y haga clic en Continuar.
Nota: Para crear un elemento de configuración sólo se requieren los valores de Nombre y Clase.
6. Introduzca los datos necesarios en los campos apropiados de la ficha Atributos.
La familia de la clase que seleccionó para el elemento de configuración determina los atributos que aparecen en la ficha. La información que introduzca aquí está determinada por los procesos empresariales y por la información que desea almacenar y visualizar para un elemento de configuración.
7. Haga clic en Guardar.
Se agrega el activo detectado.

Indicadores de activo y de CI

Hay dos indicadores de atributos comunes que pueden clasificar aún más el tipo de CI/activo con fines de filtrado y controlar qué entidades se ven en CA Service Desk Manager o en otros productos como CA APM.

Los indicadores son los siguientes:

¿Elementos de configuración (CI)? (SÍ/NO)

Identifica elementos de configuración.

Activo? (SÍ/NO)

Identifica activos.

De forma predeterminada, un elemento de configuración creado por CA CMDB está indicado como elemento de configuración, no como activo. Puede anular esto si es necesario. Un CI también puede ser un activo. CA CMDB no permite que se cambie el indicador de activo una vez que se haya configurado en Sí. Por lo general, el indicador de Activo se configura en Sí cuando CA APM ha creado un activo.

Estos indicadores aparecen en todos los formularios de detalles del CI y en la funcionalidad de búsqueda de CI. Los valores se pueden actualizar en el formulario de detalles del CI, en GRLoader y en los servicios Web de CA CMDB. La función Editar en lista también admite la actualización de los indicadores nuevos en varios registros.

El nombre de atributo de objeto para el indicador de CI es **is_ci**. El nombre de atributo de objeto para el indicador de activo es **is_asset**. Estos nombres son atributos de SREL que hacen referencia a bool. Estos nombres de atributo pueden ser utilizados como etiquetas XML de GRLoader. Por ejemplo, para cambiar el valor predeterminado del indicador Activo cuando se crea un CI con GRLoader, agregue el siguiente XML para definir el CI nuevo:

```
<is_asset>Sí</is_asset>
```

Conciliación de elementos de configuración

La reconciliación ayuda a garantizar que las actualizaciones de varios orígenes de datos que hacen referencia al mismo objeto de negocio actualizan solamente un elemento de configuración (CI), incluso aunque contengan diferente información de identificación. *La ambigüedad* representa la posibilidad de que un CI no sea único. Un CI puede tener posibles "duplicados" en la CMDB, y las transacciones de CI pueden tener más de un posible CI de objetivo. Los elementos de configuración ambiguos pueden resultar en una CMDB incorrecta, que anula el valor de la CMDB y puede llevar a acciones de negocios inapropiadas.

La reconciliación automática de elementos de configuración es una ventaja clave de CA CMDB, que ahorra una cantidad de tiempo significativa en comparación con el mantenimiento de datos manual. El proceso de reconciliar CI utiliza varios atributos de identificación específicos. Sin embargo, la reconciliación automática puede dar como resultado lo siguiente:

- Coincidencias de falso positivo
Actualización de CI existentes en lugar de crear un CI.
- Coincidencias de falso negativo
Creación de CI nuevos en lugar de actualizar un CI existente. El conjunto de CI con atributos de identificación similares es ambiguo porque se parece al mismo objeto de negocio real con atributos de identificación similares.

CA Service Desk Manager admite los siguientes enfoques de reconciliación:

Reconciliación basada en MDR (pasiva)

Permita que CMDB reconcilie los datos ambiguos según el proceso de reconciliación basada en MDR.

Identificación y resolución de CI ambiguos (reactiva)

Identifique y resuelva CI ambiguos mediante la identificación y gestión de CI existentes en CMDB.

Revise y modifique los datos entrantes mediante un área de trabajo de la transacción (proactiva)

Revise y modifique los datos entrantes antes de cargarlos en CMDB mediante un área de trabajo de la transacción (ATT).

Cada enfoque tiene ventajas e inconvenientes.

Más información:

[Reconciliación basada en MDR](#) (en la página 556)

[Identificación y resolución de CI ambiguos](#) (en la página 558)

[Revisión y modificación de datos de entrada con el área de trabajo de transacciones \(ATT\)](#) (en la página 570)

Reconciliación basada en MDR

La *reconciliación basada en MDR* se realiza en el repositorio de datos de gestión, para reducir más la ocurrencia de varios CI en el MDB que se refieren al mismo objeto en el mundo físico.

La reconciliación basada en MDR trata al MDR como una fuente de confianza que siempre utiliza el mismo ID de activo federado cuando comunica información sobre un único CI. Todas las actualizaciones de un MDR dado a un ID de activo federado dado siempre actualizan el mismo CI, incluso cuando los atributos identificatorios cambian.

La reconciliación basada en MDR, la gestión de reconciliación y el área de trabajo de transiciones (ATT) descritos en esta sección le permiten tomar el control del proceso de reconciliación. Sin embargo, para utilizar la gestión de reconciliación y el ATT satisfactoriamente, primero debe entender cómo CA Service Desk Manager utiliza los atributos de reconciliación.

Importante: si reinstala o reinicializa cualquier proveedor de datos externo (por ejemplo, CA Cohesion ACM), desactive y vuelva a activar su definición de MDR en la CMDDB. Si el MDR reutiliza sus ID de activo federado, se puede producir una superposición accidental de datos de CI.

Más información:

[Metodología de reconciliación de MDR](#) (en la página 556)

[Atributos de reconciliación de MDR](#) (en la página 557)

Metodología de reconciliación de MDR

La reconciliación basada en MDR utiliza el siguiente proceso para identificar el CI coincidente apropiado:

1. Si la transacción especifica un ID, se identifica el elemento de configuración y la reconciliación está completada.
2. Si la transacción no especifica un ID, CA Service Desk Manager comprueba si se han especificado los atributos de identificación federados y si coinciden con un CI. Si hay una coincidencia, la transacción concilia el elemento de configuración coincidente.

3. Si la transacción no especifica un ID o atributos de identificación federados, la transacción de CI utiliza los atributos de identificación descritos en la sección siguiente.

Atributos de reconciliación de MDR

La reconciliación basada en MDR utiliza la precedencia siguiente para identificar uno CI:

1. ID (si una transacción especifica un ID, la reconciliación es correcta)
2. Atributos de identificación federada
 - ID del activo federado
 - nombre de MDR
 - Clase de MDR
3. Atributos identificatorios de CI
 - Cliente (si el multiclente está instalado)
 - Nombre
 - Número de serie
 - Dirección MAC
 - Nombre de sistema
 - ID del activo alternativo
 - Nombre de DNS

Identificación y resolución de CI ambiguos

Se recomienda gestionar la ambigüedad CI por CI. En cada caso, el Administrador de configuración debe detectar cuándo existe ambigüedad y determinar el enfoque óptimo. CA Service Desk Manager usa un enfoque amplio para identificar y gestionar elementos de configuración ambiguos que ya se encuentran en la CMDB.

El *índice de ambigüedades* es una medida operativa de la no unicidad potencial de un elemento de configuración (CI), que se basa en sus atributos identificadores. El índice de ambigüedades puede medir la probabilidad de elementos de configuración "duplicados" en la CMDB o la probabilidad de que una transacción pueda tener varios objetivos de CI.

Utilice el siguiente proceso para identificar y resolver CI ambiguos:

1. Identifique CI ambiguos.
 - Cálculo del índice de ambigüedades para todos los CI
 - Revisión de la lista de CI ambiguos en el panel de resultados
2. Determine si los atributos de identificación de cada CI son válidos.
3. Resuelva el CI ambiguo con una de las siguientes acciones:
 - Modificación de los atributos de identificación
 - Exclusión de un CI de la gestión de ambigüedad
 - Rechazo de una actualización de CI mediante la desactivación del CI
 - Reemplazo de un CI

Más información:

[Ejemplo de ambigüedad de CI](#) (en la página 558)

[Cómo identificar CI ambiguos y determinar si sus atributos de identificación son válidos](#) (en la página 560)

[Cómo resolver CI ambiguos](#) (en la página 567)

Ejemplo de ambigüedad de CI

En CMDB, se cargan los datos de cuatro orígenes de datos. Cada origen de datos utiliza su propio subconjunto de características de identificación. Debido a esta incoherencia, existen más CI en CMDB de lo que se desea.

A continuación, se indican algunos ejemplos de ambigüedad de CI:

Ejemplo: elementos de configuración ambiguos

Los siguientes cuatro elementos de configuración residen en la CMDB:

- Nombre(servidor1) Nombre DNS(dns1) Número de serie(serie1)
- Nombre(servidor1) Nombre DNS(dns1)
- Nombre(servidor2) Nombre DNS(dns1) Número de serie(serie1)
- Nombre(servidor3) Dirección MAC(mac1)

Debido a las características de identificación compartidas, las dos instancias de servidor1 y servidor2 son ambiguas entre sí. Servidor3 no es ambiguo.

Cada CI tiene un índice de ambigüedades asociado a él. El índice de ambigüedades es aproximadamente la cantidad de CI existentes que coinciden con cualquiera de los atributos de identificación. Cuanto mayor sea el índice, más serán los CI que coinciden con los identificadores y, por lo tanto, mayor será la probabilidad de que se hayan introducido datos de CI inconsistentemente y que los CI adicionales se creen incorrectamente. Los CI con un índice de ambigüedades igual a cero son únicos a través de todos los identificadores y son, por lo tanto, inequívocos.

El índice de ambigüedades de cada uno de los CI anteriores es

- Primera instancia para servidor1: recuento de otros CI que coinciden con el nombre + nombre DNS + número de serie = $1+2+1=4$
- Segunda instancia para servidor1: recuento de otros CI que coinciden con el nombre + nombre DNS = $1+2=3$
- Servidor2: recuento de otros CI que coinciden con el nombre + nombre DNS + número de serie = $0+2+1=3$
- Servidor3: recuento de otros CI que coinciden con el nombre + dirección MAC = $0+0=0$

Más información:

[Cómo calcular el índice de ambigüedades](#) (en la página 561)

[Cómo ver CI ambiguos desde la ficha Administración](#) (en la página 565)

[Cómo ver CI ambiguos desde el panel de resultados](#) (en la página 566)

Cómo identificar CI ambiguos y determinar si sus atributos de identificación son válidos

Investigue cualquier CI con un índice de ambigüedades distinto a cero para determinar si es único o si se creó de forma involuntaria debido a una reconciliación incorrecta. Los CI no son ambiguos por sí mismos, son ambiguos con otros CI. Un sistema puede tener muchos conjuntos de CI ambiguos, de los cuales cada uno contiene elementos de configuración con valores comunes para los atributos de identificación.

Cuando investiga la ambigüedad de un CI, también investiga la ambigüedad de otros CI en el mismo conjunto. Cuando resuelve la ambigüedad de un CI único, reduce o elimina la ambigüedad de otros CI en ese conjunto.

CA Service Desk Manager tiene herramientas de gestión de reconciliación que permiten encontrar CI ambiguos y el conjunto de CI del que los CI ambiguos son miembros. Puede investigar la causa subyacente de la ambigüedad y resolverla.

Al gestionar ambigüedad, realice lo siguiente:

1. Calcule el índice de ambigüedades para todos los CI.
2. Utilice el panel de resultados para ver la lista de CI ambiguos. El panel de resultados enumera todos los CI que son ambiguos, en orden descendente de ambigüedad.
3. Iniciando con el CI que tiene el nivel más alto de ambigüedad en el panel de resultados,
 - a. inspeccione todos los CI en su conjunto de ambigüedad. La ficha reconciliación en el formulario de detalles de elementos de configuración de un único CI enumera el resto de los CI en el conjunto de ambigüedad.
 - b. Determine si todos los CI en el conjunto son legítimos o si hubo un error en la reconciliación. Revise los atributos de identificación y determine si los CI en el conjunto están creados de manera correcta o si se crearon debido a una coincidencia de reconciliación de falsos negativos.
4. Determine qué elementos de configuración del conjunto, si los hay, son falsos negativos.

Una vez que haya determinado que se produjo una coincidencia de reconciliación de falsos negativos y que se crearon CI adicionales, determine cuál es el CI válido y cuáles se crearon de forma incorrecta. Tenga en cuenta factores como atributos de identificación y otros atributos como la última fecha de actualización, problemas relacionados, incidencias y otros aspectos del CI.

Cómo calcular el índice de ambigüedades

Antes de poder empezar a gestionar la ambigüedad, actualice el índice de ambigüedades para los CI y las transacciones de CI existentes. El índice de ambigüedades para CI y transacciones de CI se actualiza mediante la ejecución del comando `cmdb_update_ambiguity`.

Importante: debe ejecutar `cmdb_update_ambiguity` por lo menos una vez para medir la ambigüedad de CI o transacciones de CI. Si no ejecuta el comando, todos los índices de ambigüedades son 0 (cero), lo que implica que no hay ambigüedades.

La utilidad se puede ejecutar antes y durante la gestión de ambigüedad. Planifique la utilidad para que se ejecute periódicamente, para que los índices de ambigüedades reflejen el estado actual del sistema.

Procedimiento para utilizar el índice de ambigüedades

1. Determine los parámetros necesarios para ejecutar la utilidad.
2. Ejecute la utilidad.
3. Inicie el cliente Web de CA Service Desk Manager y vaya a las listas CI ambiguo o Transacción de CI ambigua para gestionar la ambigüedad.

Comando `cmdb_update_ambiguity`

Puede calcular índices de ambigüedades de CI y de transacciones de CI si introduce una sintaxis de comando similar a la siguiente:

```
cmdb_update_ambiguity [parameters] -m { ci | twa | all }
```

Para obtener información sobre parámetros de comando, vea Parámetros `cmdb_update_ambiguity` (see page 563).

De forma predeterminada, la exploración de CI se hace a partir de la última fecha de exploración. Si se especifica "-full 1", se realiza una exploración completa.

Ejemplo: cálculo de la ambigüedad de CI en una base de datos de Microsoft SQL Server

El siguiente comando calcula el índice de ambigüedades para todos los CI y transacciones existentes en el ATT:

```
cmdb_update_ambiguity -m all -d MSSQL -u servicedesk -p dbpassword -s dbserver1
```

Ejemplo: cálculo de la ambigüedad de CI en una base de datos de Oracle

El siguiente comando calcula el índice de ambigüedades para los CI y especifica la información de la base de datos.

```
cmdb_update_ambiguity -m ci -d Oracle -u mdbadmin -p dbpassword -s server1 -port 1521 -SID orc1
```

Cómo utilizar un archivo de configuración

Puede especificar muchos parámetros `cmdb_update_ambiguity` en un archivo de configuración. Puede utilizar el archivo de configuración para proteger la configuración de parámetros en un formulario cifrado que utiliza herramientas de sistema operativo. Las palabras clave válidas y las opciones de línea de comandos correspondientes se enumeran en la tabla de parámetros.

Nota: Si especifica un parámetro en la línea de comandos y en un archivo de configuración, el valor de la línea de comandos sustituye al valor del archivo de configuración.

Ejemplo: uso de un archivo de configuración para especificar los parámetros de una base de datos de Microsoft SQL Server

El siguiente comando ejecuta el archivo de configuración `ambiguity_mssql.cfg`.

```
cmdb_update_ambiguity -m all -c ambiguity_mssql.cfg
```

Formato del archivo de configuración

Las opciones de archivo de configuración se especifican como *palabra clave=valor*. En Windows, el separador de directorios puede ser una doble barra diagonal inversa (\\) o una sola barra diagonal (/). El nombre de ruta no se debe incluir entre comillas dobles ("").

Las palabras clave válidas y las opciones de línea de comandos correspondientes se enumeran en la tabla de parámetros.

Nota: Una marca (#) en la columna 1 inicia una línea de comentario.

Ejemplo: valores de configuración de Microsoft SQL Server

```
#Ejemplo de archivo de configuración para Microsoft SQL Server
DBType=MSSQL
DBUser=servicedesk
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=C:\\Archivos de programa\\CA\\Service Desk Manager\\log
LogLevel=ERROR
SchemaName=dbo
```

Ejemplo: parámetros de configuración de Oracle

```
#Ejemplo de archivo de configuración para Oracle
DBType=Oracle
DBUser=mdbadmin
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=/tmp/ambiguity/log
LogLevel=INFO
DBPort=1521
DBSID=orcl
SchemaName=mdbadmin
```

Parámetros cmdb_update_ambiguity

Puede especificar parámetros en la línea de comandos o en un archivo de configuración (algunos parámetros son de línea de comandos solamente). En la línea de comandos, utilice comillas (") para escribir cualquier nombre de ruta con espacios; en el archivo de configuración, no utilice comillas. Si cualquier parámetro se especifica en la línea de comandos y también en el archivo de configuración, el valor de la línea de comandos sustituye al valor del archivo de configuración.

El comando cmdb_update_ambiguity utiliza los siguientes parámetros:

Opción	Palabra clave de archivo de configuración	Valores	Notas
-m	(ninguno)	att, ci, todo	(Obligatorio) Línea de comandos solamente att = calcular ambigüedad en ATT solamente. ci = calcular ambigüedad en los CI solamente. todos = calcular ambigüedad en los CI y ATT.

-d	DBType	Oracle o MSSQL	(Obligatorio. Sólo Windows). Tipo de base de datos. En Linux/UNIX, solamente se admite Oracle y esta opción no es necesaria.
-u	DBUser	<nombre de usuario de base de datos>	(Obligatorio) Nombre de usuario de base de datos. Un nombre de usuario con espacios debe estar entre comillas dobles (por ejemplo: -u "sys como sysdba"). No se requieren las comillas en el archivo de configuración.
-p	DBPassword	<contraseña de base de datos>	(Obligatorio) Contraseña para el usuario de la base de datos. Una contraseña con espacios debe estar entre comillas dobles (por ejemplo: -p "código secreto"). No se requieren las comillas en el archivo de configuración.
-c	(ninguno)	<archivo de configuración>	(Opcional) Línea de comandos solamente Nombre de ruta completo del archivo de configuración. Si hay un espacio en el nombre de ruta, debe estar entre comillas dobles.
-log	LogLocation	<directorio para colocar el archivo de registro>	(Opcional) Directorio de archivo de registro. El valor predeterminado es el directorio NX_ROOT\log.
-level	LogLevel	INFORMACIÓN, ERROR, DEPURACIÓN	(Opcional) Nivel de detalle para escribir en el archivo de registro. El valor predeterminado es ERROR.
-s	DBHost	<nombre de servidor>	(Obligatorio) Nombre de host del servidor. Para utilizar una instancia con nombre de Microsoft SQL Server, especifique <i>servidor\instancia</i> en la línea de comandos o <i>servidor\\instancia</i> en el archivo de configuración.
-CI	CI	<uuid de CI>	(Opcional) Calcule la ambigüedad para el CI

			especificado y todos los CI que sean ambiguos con éste.
-full	(ninguno)	0,1	(Opcional) Línea de comandos solamente Optimiza el rendimiento de la exploración al considerar solamente los CI actualizados desde la última vez en que se ejecutó la utilidad. Si se configura en 1, fuerza una exploración completa de todos los CI para el cálculo del índice de ambigüedades. El valor predeterminado es 0. Este parámetro no se aplica al cálculo de la ambigüedad de las transacciones. La utilidad siempre evalúa todas las transacciones en el ATT.
-port	DBPort	<número de puerto>	(Obligatorio. sólo Oracle) Número de puerto de Oracle
-SID	DBSID	<nombre de SID>	(Obligatorio. sólo Oracle) Nombre de SID de Oracle
-h	(ninguno)		(Opcional) Imprime el mensaje de uso de ayuda.
-schema	SchemaName	<nombre de esquema de base de datos>	(Opcional) El valor predeterminado es mdbadmin para Oracle; o dbo para Microsoft SQL Server.

Cómo ver CI ambiguos desde la ficha Administración

Tras ejecutar la utilidad `cmdb_update_ambiguity`, puede ver y gestionar CI ambiguos en la ficha Administración.

Para ver CI ambiguos, en la ficha Administración, vaya a CA CMDB, Gestión de la reconciliación, CI ambiguos.

La página Lista de CI ambiguos muestra la lista de CI ambiguos que tienen un índice mayor que 0 (cero).

Nota: Al hacer clic en Borrar filtro en la página de lista de CI ambiguos o de transacciones de CI ambiguos, no se vacía el campo Argumentos de búsqueda adicionales (ambigüedad > 0).

Cómo ver CI ambiguos desde el panel de resultados

Tras ejecutar la utilidad `cmdb_update_ambiguity`, puede ver y gestionar CI ambiguos en el panel de resultados.

Procedimiento para ver CI ambiguos en el panel de resultados

1. Si está en el panel de resultados de CA Service Desk Manager, amplíe la carpeta de CMDB.
2. Vaya a Gestión de la reconciliación, CI ambiguos y haga clic en una de las siguientes opciones:
 - Todos
 - Actualizado el último día
 - Actualizado la última semana
 - Actualizado el último mes

Se muestra la lista de CI ambiguos que tienen un índice mayor que 0 (cero).

Nota: Al hacer clic en Borrar filtro en la página de lista de CI ambiguos o de transacciones de CI ambiguos, no se vacía el campo Argumentos de búsqueda adicionales (ambigüedad > 0).

Cómo resolver CI ambiguos

Tras identificar CI ambiguos y determinar si sus atributos de identificación son válidos, resuelva la ambigüedad entre los CI en el conjunto de ambigüedad mediante una o varias de las siguientes opciones:

Modificación de los atributos de identificación

Si determina que los atributos de identificación no son totales o válidos, establezca los atributos de identificación del CI de modo que el CI sea único mediante la interfaz Web, GRLoader o CMDBf.

Nota: Cuando el MDR actualiza el CI, el MDR puede deshacer los cambios de reconciliación que se realizaron de forma manual.

Exclusión de un CI de la gestión de ambigüedad

Si determina que las características de identificación de los CI son correctas y representan una ambigüedad conocida y válida, puede eliminar el CI de las listas de gestión de ambigüedad y el cálculo de ambigüedad de otros CI. Asimismo, el CI se puede marcar como no ambiguo (excluir ambigüedad).

Rechazo de una actualización de CI mediante la desactivación del CI

Cuando determina que los atributos de identificación de un CI son incorrectos y que las actualizaciones que utilizan esos atributos provocan daños en los datos, los CI se pueden desactivar para impedir futuras actualizaciones. El usuario o MDR que genera la información recibe un mensaje de error y se rechaza toda la transacción.

Reemplazo de un CI

A veces las actualizaciones de la CMDB están fuera del control del administrador y los datos de identificación no válidos necesitan estar en el sistema con datos de atributo válidos que no sean de identificación. Los datos de atributo de transacción entrantes se pueden redireccionar de forma transparente a un CI reemplazado.

Nota: El redireccionamiento transparente de datos de atributo de un CI a otro puede causar confusión porque es posible que los datos de transacción no se almacenen en el mismo CI como los atributos de identificación de las transacciones podrían inducirlo a creer. Utilice este método con criterio, cuando los métodos anteriores no se pueden utilizar.

Cómo excluir elementos de configuración de la gestión de ambigüedad

A veces se reconoce que aunque un elemento de configuración particular recibe un índice de ambigüedades mayor que cero, debería quedarse tal y como está. Los elementos de configuración que tienen activada la casilla de verificación Excluir ambigüedad no se consideran parte del índice de ambigüedades o las opciones de gestión de ambigüedad.

Exclusión de ambigüedad de un elemento de configuración

Puede actualizar la opción para excluir la ambigüedad de un elemento de configuración en la interfaz Web.

Procedimiento para excluir la ambigüedad de un elemento de configuración

1. Seleccione el CI que desee eliminar de la gestión de ambigüedad en la página Lista de CI ambiguos.

Aparecerá la página de detalles del elemento de configuración.

2. Haga clic en Editar.

Aparecerá la página Actualización del elemento de configuración.

3. Active la casilla de verificación Excluir ambigüedad en la ficha Reconciliación y, a continuación, haga clic en Guardar.

El elemento de configuración se excluye del cálculo de índice de ambigüedades y otras opciones de gestión de ambigüedad.

Cómo excluir ambigüedad mediante GRLoader

Puede actualizar la opción para excluir la ambigüedad de un elemento de configuración mediante GRLoader para establecer el indicador not_ambiguous del elemento de configuración.

Los valores not_ambiguous son los siguientes:

SÍ (1)

Elimina el CI de la gestión de ambigüedad. El elemento de configuración se identifica como único independientemente de los atributos de identificación de otros elementos de configuración. El índice de ambigüedades del elemento de configuración permanece en cero.

NO 0 (predeterminado)

Este elemento de configuración es apto para gestión de ambigüedad. La unicidad de los atributos de identificación de los CI determina el índice de ambigüedades de este CI. Los atributos identificadores de este elemento de configuración se consideran al evaluar el índice de ambigüedades de otros elementos de configuración.

Cómo rechazar actualizaciones

Cuando un CI se marca como inactivo, no se pueden realizar actualizaciones en éste. Establezca el CI en inactivo si desea que CA CMDB rechace los datos de un CI dado (por su nombre, número de serie, dirección MAC, etc.) y desea que el MDR se entere del rechazo.

De esta manera, puede rechazar datos problemáticos inmediatamente y reflejarlo de vuelta en la fuente, donde el MDR puede corregir la entrada rechazada.

Para establecer un CI en inactivo en la interfaz Web, edite el CI, establézcalo en inactivo y haga clic en Guardar. También puede establecer un CI en Inactivo mediante GRLoader o servicios Web de CMDBf. Los CI desactivados también se pueden reactivar.

Cómo reemplazar CI ambiguos

Puede reemplazar un CI ambiguo para redireccionar datos a un CI de objetivo específico. Puede mostrar CI reemplazados que estén inactivos y se omitirán todas las actualizaciones de interfaz Web en ellos.

Nota: Las actualizaciones enviadas a CI reemplazados por servicios Web de CMDBf o GRLoader se vuelven a dirigir al CI reemplazado. Sin embargo, se omiten las actualizaciones de los atributos de identificación.

Para reemplazar un elemento de configuración ambiguo

1. Seleccione el CI que desee definir como el CI central (reemplazado) en la página Lista de CI ambiguos.

Aparecerá la página de detalles del elemento de configuración.

2. Haga clic en Editar.

Aparecerá la página Actualización del elemento de configuración.

3. Haga clic en la ficha Reconciliación.

Se muestran todos los CI que son ambiguos con el CI central.

Determine los CI que desea reemplazar por el CI central. Examine cada CI en la lista haciendo clic en cada uno para iniciar su página de detalles del elemento de configuración.

4. Seleccione uno o más elementos de configuración ambiguos que desee reemplazar con el elemento de configuración central y, a continuación, haga clic en Reemplazar.

El CI central reemplaza a los CI seleccionados.

Cómo ver CI reemplazados desde la ficha Administración

Puede ver elementos de configuración reemplazados desde la ficha Administración.

Para ver CI reemplazados en la ficha Administración, vaya a CA CMDB, Gestión de la reconciliación, CI reemplazados.

Aparecerá la lista de CI reemplazados.

Cómo ver CI reemplazados desde el panel de resultados

Puede ver elementos de configuración reemplazados en el panel de resultados.

Para ver elementos de configuración reemplazados desde el panel de resultados

1. Si está en el panel de resultados de CA Service Desk Manager, amplíe la carpeta de CMDB.
2. Expanda la carpeta Gestión de la reconciliación.
3. Haga clic en el nodo CI reemplazados.

Aparecerá la lista de CI reemplazados.

Revisión y modificación de datos de entrada con el área de trabajo de transacciones (ATT)

Puede guardar transacciones de relaciones y CI en almacenamiento intermedio antes de la ejecución, si copia los datos en el área de almacenamiento intermedio del ATT. Una vez en el área de almacenamiento intermedio, puede manipular los CI y las relaciones utilizando la interfaz Web o el SQL nativo.

También puede validar las transacciones de CI para impedir la creación de nuevos CI cuando deba actualizar un CI existente. En este enfoque, puede ver cada transacción y los CI potenciales que puede actualizar a fin de que pueda reconciliar la transacción manualmente con CI de objetivo. Asimismo, se pueden validar transacciones de relaciones para que hagan referencia a los CI correctos.

El *índice de ambigüedades* es una medida operativa de la no unicidad potencial de un elemento de configuración (CI), que se basa en sus atributos identificadores. El índice de ambigüedades puede medir la probabilidad de elementos de configuración "duplicados" en la CMDB o la probabilidad de que una transacción pueda tener varios objetivos de CI.

Revise y modifique transacciones de CI ambiguos mediante el siguiente proceso:

1. Identifique transacciones de CI ambiguos.
 - Cálculo del índice de ambigüedades para todas las transacciones de CI
 - Revisión de la lista de transacciones de CI ambiguos en el panel de resultados
2. Determine si los atributos de identificación de cada transacción de CI se reconcilian con el CI previsto.
3. Resuelva las transacciones de CI ambiguos con una de las siguientes acciones:
 - Modificación de los atributos de identificación
 - Especificación del CI de objetivo

Más información:

[Ejemplo de ambigüedad de transacción de CI](#) (en la página 572)
[Cómo identificar una transacción de CI ambiguos](#) (en la página 574)
[Cómo resolver transacciones de CI ambiguos](#) (en la página 575)
[Gestión de transacciones guardadas en almacenamiento intermedio](#) (en la página 576)
[Área de trabajo de la transacción](#) (en la página 577)
[Rellenar el área de trabajo de la transacción](#) (en la página 579)
[Cómo utilizar la interfaz Web para actualizar datos en el ATT](#) (en la página 591)
[Reconciliación manual](#) (en la página 593)
[Cómo cargar transacciones en el CMDB](#) (en la página 595)
[Administración del ATT](#) (en la página 597)

Ejemplo de ambigüedad de transacción de CI

Los datos de transacción de diferentes orígenes de datos se cargan en CA CMDB. Cada origen de datos utiliza su propio subconjunto de características de identificación y puede que no identifique completamente los CI de objetivo para las transacciones. A causa de esta incoherencia, puede que existan más transacciones de CI en CA CMDB de las que son válidas.

A continuación se muestra un ejemplo de la ambigüedad de transacción de CI:

Ejemplo: transacciones de CI ambiguos

La siguiente transacción de CI reside en el ATT:

- Nombre(Servidor1), nombre DNS(dns1), número de serie(serie1)

Los siguientes elementos de configuración residen en CA CMDB:

- Nombre(Servidor2), nombre DNS(dns1)
- Nombre(Servidor3), nombre DNS(dns1), número de serie(serie1)
- Nombre(Servidor4), dirección MAC(mac1), número de serie(serie1)

Debido a características de identificación compartidas, la transacción de Servidor1 es ambigua con Servidor2, Servidor3 y Servidor4 en CA CMDB.

Cada transacción de CI tiene un índice de ambigüedades asociado con él. El índice de ambigüedades es aproximadamente el número de CI existentes que coinciden en cualquiera de los atributos de identificación, menos uno, especificado en la transacción de CI. Cuanto mayor sea el índice, mayor será el número de otros CI que coinciden en los identificadores de transacción y, por lo tanto, mayor será la probabilidad que los datos de CI se hayan introducido de forma incoherente y la posibilidad de que los CI adicionales se creen incorrectamente. Las transacciones de CI con un índice de ambigüedades de cero tienen atributos de identificación que son únicos para todos los CI o tienen un CI de objetivo especificado y, por lo tanto, son inequívocos.

Ejemplo: cálculo del índice de ambigüedades

Las siguientes transacciones de CI residen en el ATT:

- Nombre(Servidor1), nombre DNS(dns1), número de serie(serie1)
- Nombre(Servidor2), nombre DNS(dns1), número de serie(serie1)

Los siguientes elementos de configuración residen en CA CMDB:

- Nombre(Servidor1), nombre DNS(dns1), número de serie(serie1)
- Nombre(Servidor2), nombre DNS(dns1), número de serie(serie1), dirección MAC(mac1)

La ambigüedad de la primera transacción (Servidor1) es 0 porque hay una coincidencia exacta con los atributos de identificación de los elementos de configuración Servidor1. El único CI de objetivo posible para esta transacción es el elemento de configuración Servidor1.

La segunda transacción (Servidor2) es ambigua con el CI Servidor1 y el CI Servidor2.

El índice de ambigüedades para las transacciones de Servidor2 consta de los siguientes componentes:

- Número de CI coincidentes con nombre (Servidor2) = 1
- Número de CI coincidentes con nombre DNS (dns1) = 2
- Número de CI coincidentes con número de serie (serie1) = 2

Según las características de identificación compartidas de CI, el índice de ambigüedades para la transacción de servidor2 es $(1-1) + (2-1) + (2-1) = 2$

Cómo identificar una transacción de CI ambiguos

Revise y modifique transacciones que tienen objetivos de CI ambiguos antes de cargar los datos de transacción. También puede resolver transacciones de elementos de configuración que no tengan un CI de objetivo pero sí atributos de identificación para uno o más elementos de configuración existentes. Este paso de resolución verifica que el elemento de configuración apropiado esté actualizado y evita que se creen datos incorrectos o incoherentes.

La ficha Reconciliación en la página de detalles de transacciones de CI enumera todos los CI que son ambiguos con esta transacción de CI central. Inspeccione los atributos de CI como la última fecha de actualización, problemas relacionados, incidencias y otros aspectos del CI para identificar el CI de objetivo que corresponde a la transacción.

Nota: Para ver la ambigüedad de los CI o las transacciones de CI, debe calcular el índice de ambigüedades mediante la utilidad `cmdb_update_ambiguity` (see page 561).

Para obtener más información, consulte Revisión y modificación de datos de entrada con el área de trabajo de transacciones (ATT). (see page 570)

Cómo ver transacciones ambiguas desde la ficha Administración

Puede ver y gestionar transacciones ambiguas desde la ficha Administración.

Para ver transacciones ambiguas, en la ficha Administración, vaya a CA CMDB, Gestión de la reconciliación, Transacciones de CI ambiguos.

Se muestra la lista de transacciones de elementos de configuración que tienen un índice mayor que 0 (cero).

Nota: Al hacer clic en Borrar filtro en la página de lista de CI ambiguos o de transacciones de CI ambiguos, no se vacía el campo Argumentos de búsqueda adicionales (ambigüedad > 0).

Cómo ver transacciones ambiguas desde el panel de resultados

Puede ver y gestionar transacciones ambiguas desde el panel de resultados.

Para ver transacciones ambiguas desde el panel de resultados

1. Si está en el panel de resultados de CA Service Desk Manager, amplíe la carpeta de CMDB.
2. Vaya a Gestión de la reconciliación, Transacciones de CI ambiguos y haga clic en una de las siguientes opciones:
 - Todos
 - Actualizado el último día
 - Actualizado la última semana
 - Actualizado el último mes

Se muestra la lista de transacciones de elementos de configuración ambiguas que tienen un índice mayor que 0 (cero).

Nota: Al hacer clic en Borrar filtro en la página de lista de CI ambiguos o de transacciones de CI ambiguos, no se vacía el campo Argumentos de búsqueda adicionales (ambigüedad > 0).

Cómo resolver transacciones de CI ambiguos

Tras identificar transacciones de CI ambiguos y determinar si sus atributos de identificación o el CI de objetivo son válidos, resuelva la ambigüedad en la transacción de CI mediante una o varias de las siguientes opciones:

Modificación de los atributos de identificación

Si determina que los atributos de identificación no son totales o válidos, puede establecer los atributos de identificación del CI de modo que el CI sea único mediante la interfaz Web.

Especificación del CI de objetivo

Si determina que el CI de objetivo no está establecido o no es válido, puede especificar un CI para una transacción ambigua a fin de que sus datos se dirijan a un CI de objetivo específico sin tener en cuenta los valores de los atributos de identificación especificados en la transacción.

Especificación de un CI de objetivo para una transacción de CI ambiguos

Puede especificar un CI para una transacción ambigua a fin de que sus datos se dirijan a un CI de objetivo específico sin tener en cuenta los valores de los atributos de identificación especificados en la transacción.

Procedimiento para especificar el CI de objetivo para una transacción de CI ambiguos

1. Seleccione una transacción de CI en la página Lista de transacciones ambiguas.

Aparecerá la página Detalles de transacción de elemento de configuración.

2. Haga clic en Editar.

Aparecerá la página Actualizar transacción de elemento de configuración.

3. En la ficha Reconciliación, seleccione un CI de la lista para designar el CI como el CI de objetivo de la transacción. Haga clic en Establecer elemento de configuración de objetivo y, a continuación, haga clic en Guardar.

El elemento de configuración seleccionado se convierte en el CI de objetivo para la transacción.

Gestión de transacciones guardadas en almacenamiento intermedio

CA CMDB proporciona una funcionalidad en la que puede almacenar datos antes de cargarlos en CA CMDB. Estos datos "guardados en almacenamiento intermedio" se almacenan como transacciones en el área de trabajo de transacciones (ATT). Una transacción guardada en almacenamiento intermedio es una unidad de trabajo que crea o actualiza un CI o relación. El ATT puede contener muchas transacciones para una relación o CI dado.

Es posible capturar datos que se estén cargando en la CMDB antes de confirmarlos para que se pueda modificar lo siguiente:

- Se pueden limpiar y normalizar los datos no estandarizados.
- Se pueden completar los datos incompletos. Por ejemplo, los nombres de elementos de configuración que empiecen por "NY" pueden tener su ubicación establecida como "New York".
- Se pueden modificar Los datos que no coincidan con las tablas de búsqueda existentes (SREL).
- Se pueden programar las transacciones para que se implementen en un futuro.

- Reconcilie transacciones en CI existentes en la CA CMDB antes de cargar los datos.
- Valide las transacciones de relaciones y CI para impedir la creación de datos no válidos o CI nuevos cuando un CI existente o único deba actualizarse. Vea cada transacción y los CI potenciales que es posible actualizar a fin de que pueda reconciliar la transacción manualmente con el CI de objetivo.

Puede utilizar el ATT para gestionar de forma proactiva el proceso de reconciliación. Puede configurar GRLoader para cargar los datos en el ATT, donde CA CMDB le permite modificar los datos de transacción para tratar transacciones que pueden crear potencialmente actualización o referencia a un CI incorrecto.

Para obtener más información, consulte Revisión y modificación de datos de entrada con el área de trabajo de transacciones (ATT). (see page 570)

Área de trabajo de la transacción

CA Service Desk Manager proporciona el área de trabajo de transacciones (ATT) para inspeccionar y modificar los datos de relación y CI antes de cargar los datos en CMDB.

El proceso de generación del ATT funciona del siguiente modo:

1. Cargue los datos (see page 579) en el ATT. El contenido puede incluir transacciones de elementos de configuración o transacciones de relaciones. El proceso de entrada no intenta reconciliar registros; simplemente rellena el área de trabajo con CI y registros de transacciones de relaciones de una de las siguientes formas:
 - GRLoader: lee los datos de XML y los almacena en el ATT mediante las opciones `-littwa` o `-littwar`.
 - SQL nativo: guarda los datos en el ATT mediante el procesamiento de SQL estándar.
 - Cree una transacción de CI o una transacción de relaciones mediante la interfaz Web.

2. (Opcional) Reconcilie manualmente las transacciones con los CI existentes en CMDB antes de cargar los datos. También se puede simular la carga de los datos (see page 584) para predeterminar si un conjunto de transacciones puede crear relaciones o CI nuevos (y por lo tanto crear nuevas ambigüedades para otros CI).

Para obtener más información, consulte Revise y modifique los datos entrantes mediante un área de trabajo de la transacción (ATT) (see page 570).

3. Modifique los datos. Puede modificar el ATT desde los siguientes orígenes:

Interfaz de usuario de CA Service Desk Manager

La interfaz de usuario basada en Web permite ver y modificar transacciones en el área de trabajo.

SQL nativo

Al ejecutar muchos cambios en varias transacciones, el SQL nativo puede modificar los datos en el ATT.

Nota: Los cambios realizados con SQL nativo pueden omitir toda la seguridad de CA Service Desk Manager.

4. GRLoader carga los datos del ATT en CA CMDB mediante las opciones -lftwa o -lftwai. Cada fila del ATT se trata como una transacción por separado.
 1. Si hay un error después de ejecutar GRLoader, el código de error se adjunta a la transacción para indicar que está incompleta (para facilitar futuros reintentos).
 2. Los registros restantes se identifican como transacciones completadas.
5. Revise los resultados de transacción y corrija los errores mediante la interfaz Web. Repita los pasos 3 y 4 según corresponda.

Tenga en cuenta lo siguiente:

- Si creó atributos o familias personalizadas y desea que sus columnas aparezcan en el área de trabajo, modifique el área de trabajo para que incluya las columnas personalizadas. Para obtener más información, consulte Ampliación del objeto ATT (see page 598).
- Utilice la última versión de GRLoader para sacar provecho del ATT. Si está utilizando un producto que incluye una versión anterior de GRLoader, actualice GRLoader a la última versión.
- Los cambios realizados a las transacciones del ATT no se auditan.

Rellenar el área de trabajo de la transacción

Usted es responsable de rellenar el área de trabajo de la transacción. Recomendamos que contacte con los servicios de CA para obtener asistencia en este proceso.

Los datos de entrada pueden proceder de diferentes fuentes, entre las que se incluyen:

- Productos de CA como CA Cohesion ACM y CA Spectrum, que importan datos mediante GRLoader
- Cualquier otro MDR que importa datos mediante GRLoader
- CA CMDB (en producción)
- Hojas de cálculo de Microsoft Excel
- Tablas de base de datos
- Una herramienta ETL elegida por un distribuidor

Vea Limitaciones de la base de datos (see page 601) para obtener más información.

Cómo cargar datos en el ATT mediante GRLoader

Las siguientes opciones de GRLoader admiten los usos del ATT:

-littwa

Carga datos XML en el ATT en estado inicial.

-littwar

Carga datos XML en el ATT en estado preparado.

-lftwa

Carga transacciones en la CMDB desde el ATT.

-lftwai

Carga transacciones en la CMDB desde el ATT y desactiva las transacciones satisfactorias.

Los documentos XML de entrada de GRLoader pueden cargarse en la CMDDB o el ATT sin modificación.

La carga de datos en el área de trabajo de transiciones puede realizarse utilizando GRLoader con la opción `-littwa` (cargar al ATT). En el archivo de configuración de GRLoader:

```
grLoader.loadtotwa=yes
```

En el modo ATT, en lugar de crear CI y relaciones directamente, GRLoader introduce la información en las tablas del área de trabajo de transiciones. Después de que los datos se hayan cargado en el ATT, pueden editarse, cambiarse y verificarse. Después de que el proceso de modificación de los datos se haya completado, pueden cargarse las transacciones individuales en CMDDB utilizando `-lftwa` o `-lftwai`.

Al cargar datos de CI en CMDDB, se someten a los CI a una reconciliación automática, que, de ser satisfactoria, origina la actualización de un único CI por parte de los datos provenientes de un objeto de negocio único en CMDDB. Cuando se cargan *transacciones de CI* en el ATT, no se realiza la reconciliación automática. Pueden aparecer varias transacciones con atributos de identificación que se dirigen a un elemento de configuración único en el ATT. Las filas del ATT existentes no se actualizan cuando se agregan nuevas filas en modo ATT, ni siquiera si coinciden exactamente con un CI existente. Incluso las mismas definiciones del CI pueden aparecer varias veces en el ATT.

GRLoader valida valores de datos al cargarse desde el modo de ATT (`-lftwa` o `-lftwai`) para crear objetos en la CMDDB o al ejecutarse mediante el modo de simulación (`-simci` o `-simrel`). Si desea obtener más información, consulte *Cómo simular operaciones de ATT* (see page 584). Los valores de datos no se validan cuando GRLoader se carga al modo de ATT (`-littwa` o `-littwar`).

El parámetro `-littwai` (o la opción de configuración `grloader.loadtotwa.inactivate`) desactiva transacciones de ATT cargadas satisfactoriamente. Después de que una transacción cargada satisfactoriamente se haya marcado como inactiva, se puede borrar permanentemente del ATT utilizando el archivado/borrado definitivo.

Ejemplo: Cargar a CMDB

El comando siguiente carga los datos directamente en CMDB:

```
grloader ... -i mydata.xml -a -n
```

El archivo XML mydata.xml contiene:

```
<GRLoader>
  <ci>
    <name>servidor1</name>
    <class>Servidor</name>
  </ci>
</GRLoader>
```

Ejemplo: Cargar al ATT

El comando siguiente carga los datos en el ATT, para que pueda manipularse antes de cargarlos a CMDB:

```
grloader ... -i mydata.xml -l ttw
```

Más información:

[Entrada XML](#) (en la página 581)

[búsqueda](#) (en la página 582)

[Formato de fecha](#) (en la página 583)

[EMPTY](#) (en la página 583)

Entrada XML

GRLoader utiliza datos de entrada XML. Cuando se cargan en el ATT, las columnas XML siguientes se asignan para evitar conflictos cuando los nombres de las columnas se solapan con los nombres de las columnas estándar de la base de datos.

Nombre de fuente de XML:	Columna de destino de la base de datos
cliente	tgt_tenant
ID	tgt_id
delete_flag	tgt_delete_flag

Para relaciones, se aplica la siguiente asignación:

Nombre de fuente de XML:	Columna de destino de la base de datos
nombre	provider_name o dependent_name

dns_name	provider_dns_name o dependent_dns_name
delete_flag	tgt_delete_flag

Las asignaciones se invierten al cargar desde las tablas de la base de datos del ATT.

búsqueda

Cuando especifica los datos para los atributos de búsqueda (SREL) en el ATT, deben contar con el mismo formato que tendrían si los hubiera especificado en XML nativo para GRLoader. Los atributos de búsqueda aceptan solamente un conjunto específico de valores que se debe definir en tablas relacionadas en CA Service Desk Manager. Estos atributos pueden tener también otras restricciones y excepciones como requisito previo para la asignación. Los valores especificados son lo mismo sin importar que se especifiquen utilizando XML, SQL o la interfaz Web del ATT.

Para determinar si un atributo es un SREL, diríjase a las siguientes secciones de la *Referencia técnica de CA CMDB*:

- Familias y clases (Los atributos de SREL se identifican)
- Contacto y otros campos de búsqueda
- Campos validados con datos de tablas existentes (SREL)

Ejemplo: búsqueda XML

En el ejemplo siguiente, la columna SREL alternativa se configura mediante la especificación del parámetro de búsqueda:

```
<ci>
<name>servidor1</name>
<owner lookup="userid">mckpe99</owner>
</ci>
```

En el ATT se puede lograr lo mismo mediante la adición de la columna SREL alternativa como sufijo al valor de los datos, incluida entre delimitadores (consulte los delimitadores `grloader.workarea.delimiters` a continuación). La transacción equivalente está representada en el Área de trabajo de la transacción como:

ID	Nombre	Propietario
100	servidor1	mckpe99 {userid}

También puede establecer el carácter delimitador utilizado arriba en el archivo de configuración de grloader:

```
grloader.workarea.delimiters=xy
```

Donde x e y son caracteres diferentes que normalmente no aparecen en el área de trabajo.

Formato de fecha

GRLoader admite las siguientes opciones de formato de fecha en XML:

- datefmt=UTC
- datefmt=localtime (predeterminado)

Ejemplos: datefmt XML

```
<ci>
<name>servidor1</name>
<purchase_date datefmt="UTC"> 1241197235</purchase_date>
</ci>
```

```
<ci>
<name>servidor3</name>
<purchase_date> 2009/05/01</purchase_date>
</ci>
```

La transacción equivalente está representada en el Área de trabajo de la transacción como:

ID	Nombre	purchase_date
101	servidor1	1241197235
102	servidor2	2009/05/01

Nota: Si una fecha contiene un carácter especial como una barra (/), el formato se supone que es "localtime". Si una fecha no contiene caracteres especiales, se da por supuesto que es UTC.

EMPTY

GRLoader admite la opción `update_if_null` en XML que borra un campo en CMDDB. El ejemplo siguiente borra el campo del propietario del servidor1 Sin el atributo, el campo del propietario no se ve afectado. Al utilizar el ATT, puede utilizar la palabra clave EMPTY.

Ejemplo: update_if_null XML

```
<ci>
<name>servidor1</name>
<owner update_if_null="yes"></owner>
</ci>
```

En el ATT, se borra el valor de la base de datos si se especifica la palabra clave EMPTY como valor de cadena. La transacción equivalente en el área de trabajo es:

ID	Nombre	Propietario
102	servidor1	EMPTY

El valor de la palabra clave puede establecerse mediante la opción de configuración:

```
grloader.emptyvalue=xxxx
```

donde xxxx representa cualquier cadena que normalmente no aparece en los datos del área de trabajo.

Cómo simular operaciones de ATT

Es posible predeterminar si un conjunto de transacciones puede crear relaciones o CI nuevos (y, por lo tanto, crear nuevas ambigüedades para otros CI) mediante las siguientes opciones:

-simci

Simula el procesamiento solamente de transacciones de CI. Se puede utilizar para determinar si las transacciones crean o actualizan CI. Cuando se utiliza la opción -simci, GRLoader ejecuta la validación de datos.

-simrel

Simula el procesamiento solamente de transacciones de relaciones. Se puede utilizar para determinar si las transacciones de relaciones crean o actualizan relaciones. La opción -simrel comprueba relaciones para la existencia de CI de proveedor y CI dependientes, valida tipos de relaciones, etc.

El resultado del modo de simulación se dirige al ATT o al archivo _err.xml. En el modo de carga normal, el archivo _err.xml contiene la entrada de CI y un comentario que indica si el CI se insertó o se actualizó. Cuando se utiliza la simulación, el mensaje de GRLoader en la Lista de transacciones de CI indica si el CI o relación se insertó o se actualizó, con otros mensajes de error relevantes. El estado de transacción permanece sin cambios.

También se puede habilitar la simulación en un archivo de configuración con las opciones **grloader.simulateloadci** y **grloader.simulateloadrelation**.

Nota: Si la entrada de GRLoader crea elementos de configuración y relaciones al mismo tiempo, la opción -simrel puede procesar solamente CI reales, y no CI que se programan para crearse. A causa de esta limitación, -simci y -simrel se excluyen mutuamente.

Cómo utilizar SQL para actualizar datos en el ATT

El ATT se almacena en la MDB y puede actualizarlo directamente con consultas SQL.

Más información:

[Tablas del ATT](#) (en la página 585)

[Nombres de columna SQL de ATT](#) (en la página 586)

[Inserción de nuevos registros en el ATT](#) (en la página 588)

[Cómo usar el controlador ODBC](#) (en la página 589)

[Identificadores de CI en el ATT](#) (en la página 589)

[Cómo establecer estados de transacción](#) (en la página 590)

[Cómo compartir tablas con CA Service Desk Manager](#) (en la página 590)

Tablas del ATT

Las tablas del Área de trabajo de la transacción (ATT) incluyen:

ci_twa_ci

Una tabla única que contiene todos los atributos de todas las familias de CI. Los datos de esta tabla están almacenados en un formulario no normalizado para permitir a los clientes y servicios que entiendan y manipulen el contenido.

ci_twa_relation

Complementa la tabla ci_twa_ci. Esta tabla contiene información de relaciones de elementos de configuración.

Los nombres de la columna ATT corresponden a los atributos que se utilizan con GRLoader, con algunas excepciones.

Nota: Para obtener información sobre los atributos del CI, consulte la *Guía de referencia técnica de CA CMDB*.

Nombres de columna SQL de ATT

Los nombres de columna en las tablas `ci_twa_ci` y `ci_twa_relation` hacen coincidir los nombres de atributo de relación y CI con algunas excepciones.

Campos de ATT comunes a `ci_twa_ci` y `ci_twa_relation`

apply_after_dt (Aplicar después de la fecha)

GRLoader ejecuta la transacción solamente si la fecha actual es posterior a la fecha de aplicación. Medido en número de segundos desde el lote. Si el valor es cero (0), se ignora este campo.

tran_chg_ref_num (Orden de cambio)

Especifica el identificador de orden de cambio asociado con esta transacción. La opción `-chg` de GRLoader utiliza este atributo para seleccionar solamente transacciones con el número de orden de cambio específico.

Nota: Para obtener más información sobre el uso de la opción `-chg`, consulte el tema sobre filtrado por número de orden de cambio (see page 597).

tran_status (Estado de transacción)

Especifica que el estado de la transacción debe ser uno de los valores siguientes (se ejecutan solamente transacciones con `tran_status=1`).

Valor	Descripción corta	Descripción larga
0	Inicial	Valor predeterminado: Requiere intervención para mover a "Listo" para que GRLoader actúe en la transacción
1	Listo	La transacción está lista para cargarse en el CI apropiado o en las tablas de relación
2	Correcto	Transacción procesada con éxito
3	Advertencia	Se ha detectado una advertencia durante la carga de <code>ca_owned_resource/bmhier</code>
4	Error	Se ha detectado un error durante la carga en <code>ca_owned_resource/bmhier</code>
40000+	Para uso del usuario	

tran_message (Mensaje)

Mensaje de GRLoader que muestra los resultados de la carga o simulación.

tran_dt (Fecha de transacción)

Evita que la información actual se superponga de forma accidental a los datos de transacción anteriores. La fecha de transacción se compara con la fecha de la última modificación del CI y GRLoader rechaza la transacción si el CI es más reciente.

Si GRLoader rechaza una transacción por ser más antigua que el CI de objetivo, verifique que la transacción siga siendo pertinente y establezca la fecha de transacción manualmente para que sea más actual. A continuación, vuelva a ejecutar GRLoader.

tgt_delete_flag (¿Activo?)

Desactiva el CI de objetivo o la relación. Establezca este valor en 1 (uno). No es lo mismo que configurar delete_flag en 1, que indica que debe suprimirse la transacción.

columnas ci_twa_ci

Además de los siguientes nombres de columna, también puede especificar nombres de atributo de CI como nombres de columna en las instrucciones SQL.

tgt_id (CI de objetivo)

Especifica el UUID del CI de objetivo. Se utiliza al realizar reconciliación manual.

superseded_by (Reemplazado por)

Especifica el UUID del CI reemplazado.

tgt_tenant (Cliente)

Especifica el nombre de cliente asignado al CI de objetivo. Tenga en cuenta que el cliente sólo puede asignarse durante la creación del CI si el usuario de GRLoader dispone de la autorización adecuada. Se aplica solamente cuando el multicitente está habilitado.

columnas ci_twa_relation

Además de los siguientes nombres de columna, también puede especificar nombres de atributo de relación como nombres de columna en las instrucciones SQL.

Utilice los siguientes nombres de columna de base de datos al usar SQL para definir transacciones de relaciones:

provider_name (Nombre del proveedor)

provider_mac_address (Dirección MAC del proveedor)

provider_serial_number (Número de serie del proveedor)

provider_system_name (Nombre de host del proveedor)

provider_asset_num (Número de activo del proveedor)

provider_dns_name (Nombre de DNS del proveedor)

provider_tenant (Cliente del proveedor)

Y

dependent_name (Nombre dependiente)

dependent_mac_address (Dirección MAC dependiente)

dependent_serial_number (Número de serie dependiente)

dependent_system_name (Nombre de host dependiente)

dependent_asset_num (Número de activo dependiente)

dependent_dns_name (Nombre de DNS dependiente)

dependent_tenant (Cliente dependiente)

Si se conocen los UUID de CI dependientes o de proveedor, puede utilizar los campos siguientes:

provider_id especifica el UUID del CI de proveedor

dependent_id especifica el UUID del CI dependiente

Nota: provider_tenant y dependent_tenant solamente se aplican cuando el multicliente está habilitado.

Inserción de nuevos registros en el ATT

Puede insertar un nuevo registro en las tablas ci_twa_ci y ci_twa_relation desde fuera de CA Service Desk Manager.

Para insertar registros en las tablas ci_twa_ci y ci_twa_relation, especifique 0 en la columna ID de la siguiente forma:

```
insert into ci_twa_ci values(id, name) values(0,'test-ci');  
insert into ci_twa_relation values(id, type) values(0,'test-relation-type');
```

Precaución: Si el multicliente está habilitado, proporcione atributos de cliente, tgt_tenant, provider_tenant o dependent_tenant según corresponda. Si crea transacciones de ATT sin especificar ningún cliente, se utiliza el cliente público.

Cómo usar el controlador ODBC

Puede utilizar SQL en lugar de GRLoader para cargar el ATT. Recomendamos que utilice el controlador ODBC que se proporciona con CA Service Desk Manager, en lugar de los servicios de SQL nativo. El uso del controlador ODBC proporciona los beneficios siguientes:

- Rendimiento
- Seguridad
- Independencia de las bases de datos
- La integridad de los datos en un entorno donde puede haber actualizaciones de la base de datos que vengan del servidor de CA Service Desk Manager al mismo tiempo que se ejecuta la herramienta de edición masiva.

Precauciones

- Solamente los controladores ODBC de CA Service Desk Manager cumplen con las opciones de seguridad como multiciente, partición de datos y acceso de rol. El SQL que se ejecuta utilizando los controladores DBMS nativos no exige seguridad.
- Realice copias de seguridad de los datos con frecuencia cuando lleve a cabo actualizaciones utilizando SQL nativo.

Identificadores de CI en el ATT

En la tabla ci_twa_ci, existen tres identificadores asociados con una transacción de CI: ID, tgt_id y superseded_by. Estos atributos son:

- El ID es el número de secuencia de la transacción. **No modifique este campo.** Los ID 1-2.000.000.000 están reservados para ser utilizados por sistemas que modifican el ATT fuera del servidor de CA Service Desk Manager. Los ID desde 2.000.000.001 a aproximadamente cuatro mil millones se reservan para ser utilizados por CA Service Desk Manager. Cuando el sistema agota los ID, reinicie la tabla.
- tgt_id, provider_id, o dependent_id son el UUID del CI de objetivo. Establezca este campo siempre que ejecute la reconciliación manual.
- superseded_by es el UUID del CI de reemplazo. Configure este campo cuando designe manualmente el CI de reemplazo para la transacción.

Cómo establecer estados de transacción

Se puede configurar el estado de la transacción (tran_status) de cada transacción del ATT. Para que GRLoader procese una transacción, debe estar establecido como Listo (tran_status=1).

Valor	Descripción corta	Descripción larga
0	Inicial	Valor predeterminado: Requiere intervención para mover a Listo para que GRLoader actúe en la transacción
1	Listo	La transacción está lista para cargarse en el CI apropiado o en las tablas de relación
2	Correcto	Transacción procesada con éxito
3	Advertencia	Se ha detectado una advertencia durante la carga de ca_owned_resource/bmhier
4	Error	Se ha detectado un error durante la carga en ca_owned_resource/bmhier
40000+	Para uso del usuario	

Si se ejecuta GRLoader -lftwa dos o más veces, se actualiza el estado después de la primera ejecución y todas las ejecuciones subsiguientes no encuentran ninguna transacción. Vuelva a establecer el estado de las transacciones listas antes de cada ejecución de -lftwa de GRLoader.

Para obtener más información acerca de cómo representar datos XML en las tablas del ATT, consulte los ejemplos XML de las secciones anteriores.

Cómo compartir tablas con CA Service Desk Manager

Servidor de SQL solamente

Al utilizar SQL para actualizar las tablas ci_twa_ci y ci_twa_relation, establezca la columna de last_mod_dt manualmente, de la siguiente manera:

```
SET last_mod_dt = DATEDIFF(s, '19700101', GETUTCDATE())
```

Ejemplo: establecer last_mod_dt

En el ejemplo siguiente se establece last_mod_dt:

```
UPDATE ci_twa_ci
    SET tran_status=1,
        last_mod_dt = DATEDIFF(s, '19700101', GETUTCDATE())
    WHERE tran_status=1
```

Nota: Las actualizaciones de tablas de ATT pueden demorar varios minutos en aparecer en la interfaz Web o GRLoader. Para obtener más información acerca de los tiempos de actualización, consulte la opción NX_DBMONITOR_TIMER_MINUTES.

Cómo utilizar la interfaz Web para actualizar datos en el ATT

Puede guardar transacciones de relaciones y CI en almacenamiento intermedio antes de la ejecución, si copia los datos en el área de almacenamiento intermedio del ATT. Una vez en el área de almacenamiento intermedio, puede manipular los CI y las relaciones mediante interfaces Web.

También puede validar las transacciones de relaciones y CI para impedir la creación de datos no válidos o CI nuevos cuando un CI existente o único debería haberse actualizado. En este enfoque, puede ver cada transacción y los CI potenciales que puede actualizar a fin de que pueda reconciliar la transacción manualmente con CI de objetivo.

Para gestionar el área de trabajo de transiciones, seleccione la ficha Administración y desplácese a CA CMDB, nodo del área de trabajo de transacciones. Desde este nodo puede gestionar las páginas del área de trabajo de transacciones.

Nota: Para obtener más información, consulte la *ayuda en línea*.

Más información:

[Gestionar transacciones de CI](#) (en la página 592)

[Gestión de transacciones de CI ambiguas](#) (en la página 593)

[Reconciliación manual](#) (en la página 593)

Gestionar transacciones de CI

La página Detalles de transacción de CI muestra todos los atributos que no están vacíos en la transacción. Si desactiva la casilla de verificación Ocultar valores vacíos, se muestran todos los atributos de CI. Para obtener información adicional sobre los atributos, señale el nombre del atributo.

Dispone de estas posibilidades:

- Ver una transacción
- Creación de transacciones
- Editar la transacción
- Guardar o cancelar los cambios de la transacción (Modo de edición)
- Volver a configurar los datos de la transacción original (Modo de edición)
- Mostrar u ocultar datos (ficha Atributos)
- Establecer el CI de objetivo (ficha Reconciliación)

Después de guardar una sola transacción, haga clic en la ficha Reconciliación para que esa transacción verifique que no hay ambigüedad en su CI de objetivo previsto. Si hay ambigüedad, puede especificar un CI de objetivo (see page 576). Cuando toda la entrada de datos esté completa, puede simular una carga de los datos (see page 584) para validarlos y comprobar la reconciliación.

Importante: los datos introducidos en el ATT mediante esta interfaz Web deben seguir las reglas descritas en el sección "Cómo cargar datos en el ATT mediante GRLoader (see page 579)".

La interfaz Web no valida datos que distinguen entre mayúsculas y minúsculas en el ATT. Verifique que los valores introducidos coincidan exactamente con los valores de búsqueda. Opcionalmente, al ejecutar GRLoader, puede especificar la opción -I para habilitar búsquedas que no distinguen entre mayúsculas y minúsculas.

Nota: Aunque las tablas tgt_id o superseded_by se almacenen como UUID en la transacción, se muestran como nombres de CI en la interfaz Web.

Gestión de transacciones de CI ambiguas

Revise y modifique transacciones que tienen objetivos de CI ambiguos antes de cargar los datos de transacción. También puede resolver transacciones de elementos de configuración que no tengan un CI de objetivo pero sí atributos de identificación para uno o más elementos de configuración existentes. Esta resolución ayuda a garantizar que el elemento de configuración apropiado esté actualizado y evita que se creen datos incorrectos o incoherentes.

Después de guardar una sola transacción, haga clic en la ficha Reconciliación para que esa transacción verifique que no hay ambigüedad en su CI de objetivo previsto. Si hay ambigüedad, puede especificar un CI de objetivo (see page 576). Cuando toda la entrada de datos esté completa, puede simular una carga de los datos (see page 584) para validarlos y comprobar la reconciliación.

Para obtener más información sobre la reconciliación de datos en el ATT, consulte Revisión y modificación de datos de entrada con el área de trabajo de transacciones (ATT). (see page 570)

Reconciliación manual

Para reconciliar una transacción de CI manualmente, determine el CI de objetivo que coincide con los atributos de identificación de la transacción y configure el `tgt_id` de la transacción en el UUID del CI de objetivo.

Cuando GRLoader procesa una transacción que especifica un `tgt_id`, actualiza el CI de objetivo con la información de la transacción y vuelve a registrar ese CI cuando los atributos de identificación han cambiado.

En la transacción, se puede especificar el CI de objetivo explícitamente. También se puede utilizar la ficha Reconciliación para seleccionar un CI de objetivo.

Para obtener más información, consulte Revise y modifique los datos entrantes mediante un área de trabajo de la transacción (ATT) (see page 570).

Especificación de un CI de objetivo para una transacción de CI ambiguos

Puede especificar un CI para una transacción ambigua a fin de que sus datos se dirijan a un CI de objetivo específico sin tener en cuenta los valores de los atributos de identificación especificados en la transacción.

Procedimiento para especificar el CI de objetivo para una transacción de CI ambiguos

1. Seleccione una transacción de CI en la página Lista de transacciones ambiguas.
Aparecerá la página Detalles de transacción de elemento de configuración.
2. Haga clic en Editar.
Aparecerá la página Actualizar transacción de elemento de configuración.
3. En la ficha Reconciliación, seleccione un CI de la lista para designar el CI como el CI de objetivo de la transacción. Haga clic en Establecer elemento de configuración de objetivo y, a continuación, haga clic en Guardar.
El elemento de configuración seleccionado se convierte en el CI de objetivo para la transacción.

Gestionar transacciones de relaciones

La lista de transacciones de relación muestra la entrada de datos en la transacción de relaciones.

A través de esta página, puede realizar lo siguiente:

- Buscar transacciones de relaciones

En la lista, puede realizar lo siguiente:

- Crear una transacción de relaciones
- Editar en lista (excepto los atributos de identificación)

Actualización de transacciones de relaciones

Puede ver y modificar los datos para una única transacción de relaciones. En la página Detalles de la transacción de relación, puede realizar lo siguiente:

- Crear una transacción de relaciones
- Ver la transacción
- Editar la transacción
- Guardar o cancelar los cambios de la transacción (Modo de edición)
- Volver a configurar los datos de la transacción original (Modo de edición)

Para actualizar una transacción de relaciones

1. Haga clic en Editar.
Aparece la página Actualizar transacción de relación.
2. Modifique y complete los campos.
3. Seleccione el activo.
4. Haga clic en Guardar.
Se guarda la transacción de relaciones.

Cuando toda la entrada de datos esté completa, puede simular una carga de los datos para validarlos y comprobar la reconciliación.

Importante: los datos introducidos en el ATT mediante esta interfaz Web deben seguir las reglas descritas en el sección "Cómo cargar datos en el ATT mediante GRLoader (see page 579)".

La interfaz Web no valida datos que distinguen entre mayúsculas y minúsculas en el ATT. Verifique que los valores introducidos coincidan exactamente con los valores de búsqueda. Opcionalmente, al ejecutar GRLoader, puede especificar la opción -I para habilitar búsquedas que no distinguen entre mayúsculas y minúsculas.

Nota: Aunque las tablas provider_id o dependent_id se almacenen como UUID en la transacción, se muestran como nombres de CI en la interfaz Web.

Cómo cargar transacciones en el CMDB

En lugar de utilizar la entrada XML para crear CI y relaciones, se pueden especificar las siguientes opciones para seleccionar ATT como su fuente de entrada.

-lftwa (cargar desde ATT)

-lftwai (cargar desde ATT y desactivar)

Nota: A diferencia de los otros modos de GRLoader que utilizan un archivo err.xml, la carga desde el ATT devuelve mensajes de error al campo de mensaje de la transacción para la visualización.

A medida que se procesan las transacciones, GRLoader configura el estado de transacción para indicar el éxito o el error de cada transacción del ATT. Si se ejecuta -lftwa de GRLoader varias veces sucesivamente, debe configurar el estado de la transacción entre las ejecuciones de GRLoader, ya que no intentará cargar datos que ya estén cargados.

La transacción se ejecuta desde el ATT como si GRLoader se estuviera ejecutando utilizando la entrada XML. La seguridad de la transacción se basa en el usuario que ejecuta la carga desde el ATT, no el usuario que cargó la transacción del ATT originalmente.

La auditoría ocurre cuando se procesan las transacciones correctamente.

Nota: Antes de ejecutar la carga, se puede predeterminar si un conjunto de transacciones creará relaciones o CI nuevos mediante las opciones de simulación (-simci y -simrel), consulte Cómo simular operaciones de ATT (see page 584) para obtener más información.

Más información:

[Cómo evitar la regresión de datos](#) (en la página 596)

[Filtrar por número de orden de cambio.](#) (en la página 597)

Cómo evitar la regresión de datos

Mientras los datos de transacción para un CI estén en el ATT, cualquier otra acción puede actualizar dicho CI en el CMDB y tornar en inválido a los datos de transacción del ATT. Para evitar que se produzca una regresión de datos no deseada, GRLoader compara el campo tran_dt (fecha de transacción) de ATT con last_update_dt (fecha de la última modificación) del CI o last_mod_dt (fecha de la última modificación) de la relación. Si last_update_dt es más reciente, GRLoader rechaza la transacción del ATT y envía un mensaje de error a la columna de tran_message.

Puede resolver esta situación realizando alguna de las siguientes acciones:

- Utilizar la interfaz Web para editar el campo del CI o de la relación tran_dt (fecha de transacción) para establecer un valor más apropiado.
- Configurar la opción de GRLoader
grloader.workarea.ignore_transaction_dates="yes" para ignorar las fechas de transacción e insertar los datos.

Nota: Si GRLoader rechaza una transacción como más antigua que el CI de objetivo y verifica que debe ejecutarse la transacción, configure la fecha de transacción manualmente para que sea más actual y vuelva a ejecutar GRLoader.

Advertencia: La opción de ignorar las fechas de transacción puede provocar que los datos vuelvan a un nivel anterior o su regresión. Cuando se actualiza un solo elemento de configuración o una relación varias veces en la misma ejecución de GRLoader -lftwa, la fecha last_update del elemento de configuración se establece en la hora actual durante la primera actualización. Para permitir varias actualizaciones del mismo CI o relación, se realiza una comprobación adicional para ver si el CI o relación se ha actualizado después de que se iniciara GRLoader. De ser así, entonces se permite la actualización.

Filtrar por número de orden de cambio.

La nueva opción de -chg de GRLoader puede utilizarse para seleccionar sólo transacciones que están asociadas a un ticket de cambio. Para poder filtrar por número de cambio, debe configurar el atributo de la orden de cambio (tran_chg_ref_num) con el número de petición de cambio apropiado.

Nota: La cadena de solicitud de cambio no se valida cuando se carga en CMDB.

Ejemplo: Filtrar por ticket de cambio

La opción siguiente carga sólo transacciones relacionadas con la orden de cambio 23434.

```
grloader -lftwa -chg 23434
```

Administración del ATT

El ATT puede requerir la siguiente administración:

- Extender el ATT: necesario cuando se extiende alguna familia de OOB o se definen las familias propias personalizadas.
- Archivado y borrado definitivo del ATT
- Cómo utilizar el ATT con CA Cohesion ACM
- Limitaciones de la base de datos

Más información:

[Extensión del objeto ATT](#) (en la página 598)

[Archivado y borrado definitivo del ATT](#) (en la página 599)

[Opciones de comandos de GRLoader de ATT](#) (en la página 599)

[Opciones del archivo de configuración de GRLoader de ATT](#) (en la página 600)

[Cómo utilizar el ATT con CA Cohesion ACM](#) (en la página 601)

[Limitaciones de la base de datos](#) (en la página 601)

Extensión del objeto ATT

Cualquier modificación en el esquema de familia de CA CMDB requiere modificaciones paralelas al esquema del ATT. Si no se han definido familias personalizadas ni atributos, el ATT no necesita modificarse.

Para extender el objeto ATT

1. Personalice las familias y los atributos definidos por el usuario utilizando los procedimientos de Extensión de CA CMDB en la *Guía de administración*.
2. Agregue los atributos de la nueva familia al esquema ci_twa_ci utilizando el diseñador de esquemas Web Screen Painter.

Para agregar un nuevo atributo al esquema ci_twa_ci:

1. Utilizando el diseñador de esquemas Web Screen Painter, abra el esquema para la tabla ci_twa_ci.
2. Agregue el atributo de familia deseado a la tabla de extensión.
3. Publique el esquema ci_twa_ci modificado.

Nota: Los nuevos atributos deben ser del tipo STRING y tener el valor de texto más largo posible.

3. Agregue los metadatos para la familia personalizada al ATT de la manera siguiente:
 1. Utilizando Web Screen Painter, abra el archivo cmdb_metadata_site_families.html.
 2. Agregue un PDM_INCLUDE para el archivo cmdb_metadata_extension.html apropiado que se creó creado para la familia personalizada.

Archivado y borrado definitivo del ATT

Para mantener el ATT, CA Service Desk Manager proporciona las siguientes reglas de archivo de archivado/borrado definitivo:

Transacciones inactivas de elemento de configuración

Archiva y borra definitivamente transacciones de CI que están marcadas para su supresión.

Transacciones correctas de elemento de configuración

Archiva y borra definitivamente transacciones de CI que se han completado correctamente.

Transacciones inactivas de relación

Archiva y borra definitivamente transacciones de relaciones que están marcadas para su supresión.

Transacciones correctas de relación

Archiva y borra definitivamente transacciones de relaciones que se han completado correctamente.

Puede seleccionar la frecuencia con que se ejecutan las reglas o si éstas se habilitan.

Puede personalizar y habilitar las reglas para el archivado y borrado definitivo del ATT. Si es usuario frecuente del ATT, tenga en cuenta las limitaciones sobre el número de registros en el ATT impuestas por el DBMS.

Si tiene que reinicializar el ATT para limpiar todos los datos en el ATT, realice lo siguiente:

- Establezca todas las transacciones en inactivas.
- Ejecute el archivado y borrado definitivo.

Importante: no utilice SQL para suprimir todos los registros en el ATT porque se suprimirán registros de encabezamiento necesarios.

Opciones de comandos de GRLoader de ATT

CA Service Desk Manager proporciona las siguientes opciones de comando para que se las use en el procesamiento del ATT de GRLoader:

-littwa

Carga XML en el estado inicial.

-littwar

Carga XML en el estado preparado.

-lftwa

Carga transacciones desde el ATT.

-lftwai

Carga transacciones desde el ATT y desactiva transacciones satisfactorias.

-chg nnnn

Utilizado con -lftwa y -lftwar. Selecciona sólo aquellas transacciones asociadas con la orden de cambio *nnnn*.

Nota: La cadena de solicitud de cambio no se valida cuando se carga en CMDB.

-I

Omitir mayúsculas y minúsculas de los atributos de búsqueda. De forma predeterminada, el texto de personalización libre de los atributos de búsqueda se procesa para distinguir entre mayúsculas y minúsculas a menos que se utilice esta opción.

-simci

Determina si las transacciones de CI pueden crear o actualizar elementos de configuración. Cuando se utiliza esta opción, GRLoader realiza una comprobación de errores únicamente con respecto a los elementos de configuración.

-simrel

Determina si las transacciones de relaciones pueden crear o actualizar relaciones. Esta opción verifica relaciones para la existencia de CI de proveedor y CI dependientes, valida tipos de relaciones, etc.

Opciones del archivo de configuración de GRLoader de ATT

CA CMDB proporciona las siguientes opciones del ATT para el archivo de configuración de GRLoader:

grloader.emptyvalue=EMPTY

grloader.loadfrommtwa=yes

grloader.loadfrommtwa.inactivatesuccessful=yes/no

grloader.loadtotwa=yes

grloader.loadtotwa.ready=yes/no


```
grloader.workarea.delimiters={ }
```

```
grloader.workarea.ignore_transaction_dates=yes
```

```
grloader.simulateloadci=yes/no
```

```
grloader.simulateloadrelation=yes/no
```

Cómo utilizar el ATT con CA Cohesion ACM

Para utilizar el ATT con el procesamiento de CA Cohesion ACM, aplique el parche RO08739 a CA Cohesion ACM r5. Este parche le permite especificar la opción -littwa en el campo Otras opciones en la ficha Exportar opciones de la definición de Informe de exportación de CA CMDB. Actualice el componente de GRLoader. Si tiene preguntas, póngase en contacto con el servicio de atención al cliente de CA.

Limitaciones de la base de datos

El ATT está sujeto a limitaciones de datos de la base de datos subyacente, de la siguiente manera:

- Cuando utilice el ATT y Microsoft SQL Server, la longitud total de una transacción de datos no debe exceder los 8060 bytes.
- Cuando utilice las utilidades dbload y pdm_load, una operación de carga se restringe a 512 columnas.
- Oracle tiene una limitación de 1000 columnas. Si personaliza CA CMDB, verifique que el número total de atributos no exceda los 1000 caracteres incluidas todas las familias (proporcionadas por CA y definidas por el usuario).
- Las limitaciones de SQL Server 2005 tal y como se describen en la siguiente tabla.

Tipo de limitación	Límite (32 bits y 64 bits)
Columnas por tabla ancha	30000
Columnas por tabla base	1024
Columnas por instrucción SELECT	4096
Bytes por fila	8060
Filas por tabla	Limitado según el almacenamiento disponible

Mantenimiento de datos de CA CMDB

Las tareas que ejecuta para mantener datos de CMDB requieren privilegios de administrador. Estas tareas incluyen cómo configurar los tipos de relaciones, clases y familias usados para gestionar información de relación y elementos de configuración.

Más información:

[Estructura de clases/familias de CA CMDB](#) (en la página 602)

[Cambio de la familia/clase de un único CI](#) (en la página 603)

[Cambio de la familia/clase de una lista de elementos de configuración](#) (en la página 603)

[Cambio de la familia/clase de elemento de configuración mediante GRLoader](#) (en la página 604)

[Ampliación de CA CMDB](#) (en la página 605)

Estructura de clases/familias de CA CMDB

CA CMDB proporciona familias de elementos de configuración predeterminadas y las clases de CI incluidas en ellas.

Nota: Para obtener información sobre la estructura de clases y familias predeterminada de CA CMDB, consulte la *Guía de referencia técnica de CA CMDB*.

Nota: Las siguientes familias base de Service Desk y CA APM no tienen sus propias tablas de extensión de CA CMDB:

- Equipo
- Contacto (como objeto base)
- Hardware
- Ubicación (como objeto base)
- Organización (como objeto base)
- Other
- Project
- Software

En CA CMDB, los elementos de configuración de estas familias base reciben páginas de detalles del elemento de configuración con algunos campos extraños y sin ficha Atributos. Para utilizar las funciones avanzadas de CA CMDB, como la posibilidad de hacer el seguimiento de atributos, control de versiones, instantáneas y líneas base específicos de la familia, se recomienda utilizar la capacidad de Cambiar familia y clase para convertir estos elementos de configuración en familias de CA CMDB.

Cambio de la familia/clase de un único CI

Puede cambiar la familia y la clase de un único CI.

Para cambiar la familia y la clase de un único CI

1. Seleccione el elemento de configuración que desee cambiar.
2. Haga clic en Editar.
Aparecerá la página Actualización del elemento de configuración.
3. Cambie el valor Clase del elemento de configuración. La clase seleccionada también determina la familia del elemento de configuración. Se puede introducir directamente un valor o hacer clic en la lupa para seleccionarlo en una lista de clases.
4. Haga clic en Guardar.
Se cambia la familia y la clase del único CI.

Cambio de la familia/clase de una lista de elementos de configuración

Puede cambiar la familia y la clase de una lista de CI.

Para cambiar la familia/clase de una lista de elementos de configuración

1. En la lista de elementos de configuración, haga clic en Mostrar filtro.
2. Rellene uno o varios campos de búsqueda para buscar los elementos de configuración que desea editar.
3. Haga clic en Buscar.
La lista de elementos de configuración se rellena con todos los elementos de configuración que coincidan con sus criterios de búsqueda.
4. En Lista, haga clic en Editar.
La lista de elementos de configuración muestra los campos que se pueden cambiar para todos los CI seleccionados.
5. Realice los cambios deseados en los campos Familia y Clase.
6. Hacer clic en Cambiar todo.
7. Haga clic en Guardar.
Cuando se actualiza la lista de elementos de configuración, éstos aparecen actualizados.

Cambio de la familia/clase de elemento de configuración mediante GRLoader

Puede cambiar la familia y la clase para un CI utilizando GRLoader.

Para cambiar la familia o la clase de un elemento de configuración mediante GRLoader

1. Cree el código XML para cambiar el atributo del elemento de configuración.
2. Utilice GRLoader para abrir el elemento de configuración que desea modificar.
3. Para cambiar el atributo de elemento de configuración, ejecute el XML mediante GRLoader.

Se cambian la familia y la clase para un CI.

Ejemplo: establecimiento de la clase de un elemento de configuración abierto a Documento

El siguiente ejemplo muestra un fragmento de XML que establece la clase de un CI abierto en *Documento*.

```
<ci>
  <name>número de documento 1
  <class>Documento
</ci>
```

Importante: No trate de actualizar los atributos de Familia y Clase de un elemento de configuración al mismo tiempo. Para cambiarlos, debe utilizar dos actualizaciones del CI independientes en dos invocaciones de GRLoader.

Ampliación de CA CMDB

CA CMDB es un sistema sumamente flexible que se puede ampliar para incluir familias, clases y atributos adicionales según las necesidades de la empresa. Los atributos nuevos pueden ser específicos de una familia o *comunes* (es decir, aplicables a todas las familias). Si bien CA CMDB ofrece familias predefinidas con numerosas clases y atributos basado en estándares del sector, algunos casos de empresa requieren la realización de una o más de las actividades siguientes:

- Ampliar una o más de las familias de CI mediante la adición de atributos nuevos. Por ejemplo, para agregar una coordenada de GPS a cada dispositivo en su ámbito de oficina, puede definir un atributo `gps_coordinate` para agregarlo a cualquier familia deseada. Si sólo necesita ampliar una familia determinada, use el creador de esquemas de Web Screen Painter para definir los atributos nuevos en la tabla de extensión existente. Asimismo, cada vez que agregue un atributo, también tendrá que modificar la página Detalles, la ficha Atributo y los formularios de metadatos que utilizan el atributo. Para obtener más información, consulte Adición de atributos de familia (see page 606).
- Amplíe todas las familias de CI agregando un atributo común. Para obtener más información, consulte Adición de atributos comunes (see page 607).
- Agregue clases nuevas a una familia existente para admitir más detalles de clasificación en el sistema. Por ejemplo, en lugar de la clase Servidor genérica, puede crear una clase independiente para cada modelo de dispositivo de servidor. Para obtener más información, consulte Definición de una clase de elementos de configuración nueva (see page 608).
- Agregue una familia nueva utilizando una tabla de extensión existente y sus atributos. Una familia nueva ofrece un método alternativo de organizar o clasificar los CI. Para obtener más información, consulte Definición de una familia de elementos de configuración nueva (see page 609).

- Si la estructura existente de la clase o la familia no corresponde a sus necesidades, puede comenzar de nuevo con un conjunto mínimo de atributos. Si quiere agregar una familia nueva mediante una tabla de extensión nueva, defina la tabla de extensión nueva y sus atributos con el creador de esquemas de Web Screen Painter y cree también los formularios que se requieren para la visualización y la actualización. Para obtener más información, consulta Construcción de un marco de atributos nuevo (see page 610).

Importante: la ampliación de CA CMDB requiere unos conocimientos especializados de estructuras de datos y tablas de CA Service Desk Manager, así como estar familiarizado con Web Screen Painter (WSP). Le recomendamos que se ponga en contacto con los servicios de CA para que le ayuden con esta actividad y también que lea y comprenda bien las secciones siguientes antes de intentar ampliar las familias y atributos de CA CMDB.

Adición de atributos de CA CMDB nuevos

La adición de un atributo de CA CMDB nuevo requiere una minuciosa planificación. CA CMDB ya ofrece numerosos atributos en sus familias y clases predefinidas, así que debe decidir si son suficientes para sus necesidades antes de considerar la personalización.

Si determina que necesita algún atributo nuevo, se recomienda actuar con cautela y preguntarse primero si necesita:

- Agregar uno o más atributos nuevos a una familia existente
- Agregar el atributo nuevo (o atributos) a más de una familia
- Agregar un atributo común nuevo, que se aplique a todas las familias

Una familia existente se puede ampliar agregándole atributos nuevos. Por ejemplo, si algunos dispositivos en el ámbito de su oficina tienen asignada una coordenada de GPS, puede agregar un atributo `gps_coordinate` a cualquier familia de CI aplicable. Para obtener más información, continúe en Adición de atributos de familia (see page 606).

Una vez identificadas las necesidades de atributos, si determina que requieren el uso de familias y clases nuevas, consulte Adición de una familia o clase de CA CMDB nueva (see page 608).

Adición de atributos de familia

Puede agregar un nuevo atributo a una o más familias existentes mediante el Creador de esquemas de Web Screen Painter, que actualiza la base de datos para incluir el nuevo atributo y también actualiza los archivos y tablas asociadas de CA Service Desk Manager. Este método es preferible a la actualización manual de tablas y archivos.

Procedimiento para agregar un atributo nuevo a una familia

1. En el Creador de esquemas de Web Screen Painter, abra el esquema que corresponde a la tabla de extensión de la familia.
2. Agregue el atributo deseado a la tabla de extensión.
3. Publique la tabla de extensión modificada.

Nota: GRLoader y el Control de versiones recogen automáticamente los atributos nuevos sin necesidad de acciones adicionales. Sin embargo, también se recomienda que habilite el inicio de sesión. El inicio de sesión es necesario para fines de auditoría y el Control de versiones habilitado para registrar todas las instantáneas.

Para activar el inicio de sesión, verifique si el valor UI_INFO del atributo está establecido como **AUDITLOG**.

Después de crear un atributo de familia nuevo, debe agregarse a cada formulario de visualización para que los usuarios puedan consultar y actualizar ese atributo y el formulario de metadatos específico a esa tabla de extensión. Para obtener más información, consulte Adición de atributos a formularios (see page 612).

Además, el Control de versiones requiere metadatos, incluida la información sobre encabezados de columna y los atributos de elementos de configuración estándar relacionados. Puede definir los metadatos nuevos para todos los atributos nuevos que ha creado; para obtener instrucciones al respecto, siga en la sección Creación de metadatos (see page 613).

Adición de atributos comunes

Los atributos comunes se almacenan en la tabla **ca_owned_resource** del objeto **nr**. Esta tabla permite la personalización de los siguientes campos:

- smag_1
- smag_2
- smag_3
- smag_4
- smag_5
- smag_6

Si necesita menos de siete atributos personalizados entre todas las familias de CI, estos campos ofrecen una solución bastante práctica.

Tal como se ofrecen, estos campos personalizados no aparecen en ningún formulario. Para permitir que los usuarios de CA CMDB vean o actualicen un campo `smag_n`, utilice Web Screen Painter (WSP) para agregarlo a cualquier formulario de visualización deseado. Todas las funciones de inicio de sesión y de GRLoader ya están activadas.

Nota: Para obtener información sobre los procedimientos del Creador de esquemas de Web Screen Painter, consulte el capítulo "Personalización" de la *Guía de implementación de CA Service Desk* y la sección Personalización de esquemas de bases de datos de la Ayuda en línea de Web Screen Painter.

Adición de una familia o clase de CA CMDB nueva

La adición de una familia de CA CMDB nueva requiere una minuciosa planificación. CA CMDB ofrece numerosas familias y clases predefinidas, así que debe decidir si son suficientes para sus necesidades antes de considerar la personalización. Si no es así, puede cumplir con algunos requisitos nuevos realizando una de las acciones siguientes:

- Definir una clase nueva en una familia existente
- Definir una familia nueva que utilice una tabla de extensión existente

Si decide que las tablas de extensión existentes no son suficientes para sus necesidades, ignore esta sección y continúe en la sección Construcción de un marco de atributos nuevo (see page 610) para crear una tabla de extensión y los formularios que requiera.

Definición de una clase de elemento de configuración nueva

Puede agregar clases nuevas para admitir niveles más altos de granularidad de clasificación. Por ejemplo, en lugar de utilizar cualquiera de las clases de CA CMDB en la familia Hardware.Servidor, puede definir clases adicionales para distintos dispositivos de servidor.

Antes de crear una clase nueva de elemento de configuración, verifique si ya existe una clase apropiada en la Lista de clases de elemento de configuración.

Nota: Si también necesita una familia nueva para controlar un conjunto nuevo de clases, ignore este tema y continúe en la sección Definición de una familia de elemento de configuración nueva (see page 609). A continuación, puede regresar y rellenar la familia nueva con las clases oportunas.

Procedimiento para definir una clase de CI con la interfaz de administración

1. Desplácese a la Lista de clases de elementos de configuración.

2. Haga clic en Crear nuevo.
Aparecerá la página Crear nueva clase de elemento de configuración.
3. Introduzca un nombre exclusivo para la nueva clase.
4. Introduzca el nombre de familia correspondiente en el campo Familia, o haga clic en el icono que hay sobre el campo para buscar una familia.
5. Verifique si el valor del campo Estado de registro es Activo.
6. Haga clic en Guardar.

La clase de elemento de configuración nueva queda definida y está lista para que se creen nuevos CI.

Definición de una familia de CI nueva

Antes de crear una familia de elementos de configuración, verifique si ya hay una familia apropiada en la Lista de familias de elementos de configuración. Si no la hay, puede crear familias nuevas como método alternativo de organizar o clasificar los CI mediante los atributos existentes.

Si la familia nueva que necesita no puede utilizar una tabla de extensión existente (ni la tabla predeterminada), lleve a cabo todos los preparativos adicionales indicados en Construcción de un marco de atributos nuevo (see page 610). La tabla de extensión nueva se puede usar para definir familias nuevas.

Procedimiento para definir una familia de CI con la interfaz de administración

1. Desplácese a la Lista de familias de elementos de configuración.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nueva familia de elementos de configuración.
3. Introduzca un nombre exclusivo para la nueva familia.
4. Verifique si el valor del campo Estado de registro es Activo.

5. En el campo Nombre de extensión, seleccione la tabla de extensión que identifica el tipo de familia que desea crear. Puede ser una tabla de extensión nueva que haya creado recientemente.

Por ejemplo, si va a añadir una familia para un tipo de hardware no especificado, seleccione `ci_hardware_other`. Este tipo garantiza que al crear nuevos elementos de configuración cuyas clases son utilizadas por la nueva familia, aparezcan los atributos apropiados en la ficha Atributos. Si no se selecciona un nombre de tabla en el campo Nombre de extensión, se utilizará la tabla predeterminada y al crear un elemento de configuración en la nueva familia sólo aparecerán los atributos predeterminados.

6. En el campo Descripción, especifique la descripción.

La descripción que introduzca se mostrará en la Lista de familias de elementos de configuración con fines informativos.

7. Haga clic en Guardar.

La familia de elementos de configuración queda definida.

Ahora que la familia nueva es definida, le puede agregar clases como se explica en Definición de una clase de elemento de configuración nueva (see page 608).

Construcción de un marco de atributos nuevo

Si ninguna de las estructuras existentes de la clase o la familia corresponde a sus necesidades, puede comenzar otra vez con un conjunto mínimo de atributos nuevos. Esto requiere la construcción de una tabla de extensión nueva y otras estructuras secundarias.

Antes de utilizar la interfaz de administración de CA CMDB para definir una familia de CI nueva basada en una tabla de extensión nueva, utilice el Creador de esquemas Web Screen Painter para crear la tabla de extensión nueva.

Para utilizar la tabla de extensión nueva, también debe crear formularios HTML nuevos para:

- Página Detalles de CI nueva
- Ficha Atributos nueva con sus atributos asociados
- Formulario de metadatos y metadatos nuevos

CA CMDB suministra plantillas que puede utilizar para crear estos formularios HTML. Las secciones siguientes ofrecen información más detallada sobre lo que hace falta.

Nota: Para obtener información sobre los procedimientos del Creador de esquemas de Web Screen Painter, consulte el capítulo "Personalización" de la *Guía de implementación de CA Service Desk* y la sección Personalización de esquemas de bases de datos de la Ayuda en línea de Web Screen Painter.

Para utilizar el marco nuevo en la interfaz de usuario de CA CMDB, defina lo siguiente:

- Una o más familias de CI que utilicen la tabla de extensión nueva
- Las clases de elementos de configuración para clasificar los CI por tipo

Los procedimientos para definir familias y clases nuevas se encuentran en la sección anterior.

Creación de una tabla de extensión nueva

Para poder definir una familia basada en una tabla de extensión nueva, debe actualizar primero la base de datos con la tabla nueva y actualizar también el esquema de CA CMDB con información sobre esa tabla.

Procedimiento para crear una tabla de extensión

1. En el Creador de esquemas de Web Screen Painter, defina la tabla de extensión y el nombre de extensión nuevos.
2. Guarde y publique la tabla de extensión nueva.

Nota: El creador de esquemas de WSP crea automáticamente el desencadenante de inicio de sesión en CA CMDB.

Continúe en la sección siguiente para crear la página Detalles de CI.

Creación de una página de detalles de CI

Hace falta una página Detalles de CI para admitir la visualización de los atributos para los CI asociados a una tabla de extensión nueva.

Procedimiento para crear la página de detalles del elemento de configuración

1. En el Creador de esquemas de Web Screen Painter, haga clic en Archivo, Nuevo y cree un formulario basado en `detail_extension.template`.
2. Guarde este formulario nuevo como **`detail_extension.html`**, donde *extension* es el nombre de la tabla de extensión.
3. Siga las instrucciones especificadas en el archivo, pero sustituyendo la cadena **`***EXTENSION***`** por el nombre de la tabla de extensión nueva (definida anteriormente).
4. Guarde el archivo con todos los cambios.

La página Detalles de CI incluye dos secciones de atributo:

- la sección de atributo común denominada `cmdb_detail.html`,
- la sección específica de la familia (la ficha Atributos) denominada `nr_cmdb_extension_tab.html`, donde *extension* es el nombre de la tabla de extensión nueva.

Continúe en la sección siguiente Creación de la ficha Atributos de CI (see page 612).

Creación de una ficha Atributos de CI

La ficha Atributos muestra los atributos específicos de la familia para un CI.

Procedimiento para crear la ficha Atributos

1. En el Editor visual de Web Screen Painter, haga clic en Archivo, Nuevo y cree un formulario basado en `nr_cmdb_extension_tab.template`.
2. Guarde este archivo como **`nr_cmdb_extension_tab.html`**, donde *extension* es el nombre de la tabla de extensión nueva.
3. Siga las instrucciones especificadas en el archivo, pero sustituyendo la cadena **`***EXTENSION***`** por el nombre de la tabla de extensión nueva (definida anteriormente).
4. Guarde y publique el archivo con todos los cambios.

Continúe en la sección siguiente para rellenar la ficha Atributos.

Adición de atributos a formularios

Después de utilizar el Creador de esquemas de Web Screen Painter para crear un atributo nuevo en una tabla de extensión, ese atributo debe agregarse a cualquier formulario que se use para fines de visualización o actualización. En el caso de atributos nuevos específicos de la familia, el único formulario que se debe cambiar es la ficha Atributos denominada **`nr_cmdb_extension_tab.html`**, donde *extension* es el nombre de la tabla de extensión. Este formulario se debe editar para incluir cualquier atributo nuevo que corresponda.

Procedimiento para editar un formulario de atributo

1. En el Editor visual de Web Screen Painter, haga clic en Archivo, Abrir para acceder al formulario oportuno.
2. Arrastre y coloque el atributo nuevo (o atributos) en el formulario.
Nota: Los formularios suministrados por CA CMDB no se prestan a la edición con el Editor visual de Web Screen Painter, por tanto, utilice el editor de texto de Web Screen Painter en la ficha Fuente.
3. Guarde el formulario y publíquelo.

Si aún no ha creado un formulario de metadatos, continúe en la sección Creación de un formulario de metadatos (see page 613). Para definir metadatos para un atributo nuevo en el formulario, continúe en la sección Creación de metadatos (see page 613).

Creación de un formulario de metadatos

Una tabla de extensión nueva requiere su propio formulario de metadatos para definir los encabezados de columna e información de elemento de configuración estándar para el Control de versiones.

Procedimiento para crear el formulario de metadatos

1. En el Editor visual de Web Screen Painter, haga clic en Archivo, Abrir para acceder a `cmdb_metadata_extension.template`.
2. Guarde el archivo como **`cmdb_metadata_extension.html`**, donde *extension* es el nombre de la tabla de extensión nueva.
3. Siga las instrucciones especificadas en el archivo, pero sustituyendo la cadena **`***EXTENSION***`** por el nombre de la tabla de extensión nueva (definida anteriormente).
4. Guarde y publique el formulario con todos los cambios.

Continúe en la sección siguiente para rellenar el formulario de metadatos.

Creación de metadatos

Los metadatos incluyen información sobre los encabezados de la columna de atributos e información de elemento de configuración estándar que la función Control de versiones requiere.

Importante: Los metadatos requieren una planificación minuciosa para garantizar unos datos correctos en Instantáneas, unos títulos correctos en el Control de versiones y unas comparaciones satisfactorias de los elementos de configuración estándar.

Procedimiento para crear metadatos

1. En el Editor visual de Web Screen Painter, haga clic en Archivo, Abrir para acceder a **`cmdb_metadata_extension.html`**, donde *extension* es el nombre de la tabla de extensión.
2. Siga las instrucciones especificadas en el formulario para copiar y modificar la fila indicada de cada atributo de la tabla de extensión nueva.

Nota: Los atributos siguientes, aunque son obligatorios, no necesitan metadatos:

- ID
- Last_modified_by
- Etc. (se proporcionarán más adelante)

3. Guarde y publique todos los cambios.

Si va a agregar metadatos a una familia de CA CMDB existente, los cambios de auditoría aparecerán correctamente en la ficha Control de versiones. Sin embargo, si va a definir metadatos para una tabla de extensión nueva, debe disponer de una familia y clase nuevas para los atributos; para obtener más información, consulte Adición de una familia o clase de CA CMDB nuevas (see page 608).

Ahora, las estructuras para su tabla de extensión nueva están en su sitio. Para definir una familia nueva para los atributos, continúe en la sección Definición de una familia de elementos de configuración nueva (see page 609).

Ejemplo

En este caso, se va a crear una familia **Automóvil** y una clase **Sedán** dentro de ella para llevar el seguimiento del inventario de fabricación, envíos, transporte de alquiler u otros fines. Por supuesto, también podría crear muchas otras clases de automóviles; la única finalidad de este ejemplo es servir como demostración.

Paso 1: creación de la tabla de extensión nueva

1. En el Creador de esquemas de Web Screen Painter, haga clic en Agregar tabla de extensión.
2. Introduzca un nombre para la tabla de extensión nueva. En este ejemplo, **vehicle**.

La tabla de extensión **zvehicle** se crea y se muestran sus propiedades.

Nota: La letra "z" se añade al principio de todos los nombres de tabla nuevos para distinguirlas de las tablas propias de la aplicación.

3. En la ficha Información de tabla, establezca el campo Grupo de funciones como **inventario**. Otros campos se rellenarán con los valores predeterminados.
4. Agregue información nueva de columnas y atributos según desee.
5. Guarde y publique la tabla de extensión nueva.

Paso 2: creación de una familia nueva

Procedimiento para crear una familia

1. Desplácese a la Lista de familias de elementos de configuración.
2. Haga clic en Crear nuevo.
Se muestra la página Crear nueva familia de elementos de configuración.
3. Introduzca un nombre exclusivo para la nueva familia. En este ejemplo, **Automóvil**.

4. Verifique si el valor del campo Estado de registro es Activo.
5. Seleccione el nombre de la tabla de extensión. En este ejemplo, **zvehicle**.
6. Haga clic en Guardar.

Se crea la nueva familia de elementos de configuración.

Paso 3: creación de una clase nueva

1. Desplácese a la Lista de clases de elementos de configuración.
2. Haga clic en Crear nuevo.
Se muestra la página Crear nueva clase de elemento de configuración.
3. Introduzca un nombre exclusivo para la nueva clase. En este ejemplo, **Sedán**
4. Verifique si el valor del campo Estado de registro es Activo.
5. Seleccione la familia. En este ejemplo, **Automóvil**.
6. Haga clic en Guardar.

Se crea la nueva clase de elemento de configuración.

Paso 4: creación del nuevo formulario de detalles del elemento de configuración

Procedimiento para crear el formulario de detalles del elemento de configuración

1. En el Editor visual de Web Screen Painter, abra el formulario `detail_extension.template`.
2. Guarde la plantilla con el nombre **detail_zvehicle.htmlpl**.
El formulario nuevo se guarda en
`NX_ROOT\site\mods\wsp\project\web\analyst`
3. En el formulario nuevo, sustituya todas las instancias de *****EXTENSION***** por **zvehicle**
4. Guarde y publique el nuevo formulario de detalles del elemento de configuración.

Paso 5: creación de la ficha Atributos

Procedimiento para crear el formulario de la ficha Atributos

1. En el Editor visual de Web Screen Painter, abra el formulario `nr_cmdb_extension_tab.template`
2. Guarde la plantilla con el nombre **nr_cmdb_zvehicle_tab.html**
El formulario nuevo se guarda en
`NX_ROOT\site\mods\wsp\project\web\analyst`
3. En el formulario nuevo, sustituya todas las instancias de *****EXTENSION***** por **zvehicle**
4. Agregue los atributos al formulario según desee.
5. Guarde y publique el nuevo formulario de la ficha Atributos.

Paso 6: creación del formulario de metadatos

Procedimiento para crear el formulario de metadatos

1. En el Editor visual de Web Screen Painter, abra el formulario `cmdb_metadata_extension.template`
2. Guarde la plantilla con el nombre **cmdb_metadata_zvehicle.html**
El formulario nuevo se guarda en
`NX_ROOT\site\mods\wsp\project\web\analyst`
3. Sustituya todas las instancias de *****EXTENSION***** por **zvehicle**
4. Utilice los marcadores de posición de encabezado y atributo para agregar metadatos para todos los atributos específicos de la familia.
5. Guarde y publique el formulario de metadatos nuevo.

Capítulo 15: Administración de MDR

Este capítulo describe cómo definir los MDR, importar datos, reasignar elementos de configuración a su origen, definir los parámetros de inicio, volver a iniciar el MDR de origen y utilizar los MDR para asignar y visualizar información de CI federados.

Esta sección contiene los siguientes temas:

[¿Qué es un MDR?](#) (en la página 617)

[Lanzador MDR](#) (en la página 619)

[Definición de una URL para iniciar un MDR](#) (en la página 620)

[Configuración de un proveedor MDR de CA APM](#) (en la página 622)

[Inicio en contexto desde CA CMDB para CA APM](#) (en la página 623)

[Propiedades de CI que admiten la federación de MDR](#) (en la página 623)

[MDR de CA Cohesion ACM](#) (en la página 626)

[Importación de CI a CA CMDB mediante GRLoader](#) (en la página 630)

[Restricciones y convenciones de nomenclatura de los elementos de información](#) (en la página 631)

[Convención de nomenclatura `system\_name`](#) (en la página 632)

[Uso del Visor de CMDBf](#) (en la página 633)

[Cómo actualizar archivos de metadatos para la asignación de CMDBf](#) (en la página 634)

¿Qué es un MDR?

La federación de bases de datos de gestión de la configuración (CMDBf), un grupo de trabajo formado por representantes de CA, IBM, HP, Microsoft y otras compañías, define Repositorio de datos de gestión (MDR) como algo que se encarga de recopilar información sobre los elementos de configuración (CI).

Para crear la relación entre un MDR y sus elementos de configuración al implementar el lanzador MDR, realice lo siguiente:

1. Defina el MDR.
2. Defina los CI que hacen referencia a ese MDR.

No es posible tener un CI que haga referencia a un MDR inexistente, pero se puede definir un CI sin definir una asociación de MDR. Puede agregar la información del MDR durante una actualización o una edición para aprovechar todas las capacidades del lanzador MDR.

El mismo CI puede ser detectado por varios MDR. Una vez que se ha detectado el CI, cada MDR intenta gestionar ese CI; un MDR pueden realizar las acciones siguientes:

- Detectar los atributos detallados del CI.
- Intentar modificar el estado del CI.

Ejemplo: un CI detectado por varios MDR

Un CI es detectado por ambos, el software de gestión de red y un paquete de software de gestión de activos.

- El software de gestión de red mantiene la información sobre la configuración de red y la topología de red.
- El software de gestión de activos contiene la información relativa a costes, depreciación, contratos de licencia y de mantenimiento para ese CI particular.

Clases MDR y nombres MDR

Una empresa de TI puede incluir muchos MDR. Cada MDR tiene un identificador denominado *nombre MDR* (*mdr_name*). Debido a que es habitual que un MDR utilice el nombre de servidor host como su *mdr_name*, (para que varios MDR residan en el mismo servidor host), se añade una *clase de MDR* (*mdr_class*) a *mdr_name* para identificar de forma exclusiva cada MDR.

CA Cohesion ACM es una herramienta de detección empresarial que se integra muy bien con CA CMDB. Cada MDR de CA Cohesion ACM definido en CA CMDB debe tener una *mdr_class* de **Cohesion**.

Nota: Para obtener más información sobre CA Cohesion ACM, consulte la Ayuda en línea de CA Cohesion ACM. Para obtener información sobre la integración de CA Cohesion ACM y CA CMDB, consulte la *Guía de implementación de CA Cohesion ACM*.

Cómo complementa un MDR a CA Service Desk Manager

Normalmente, un MDR contiene información más detallada sobre los CI que CA CMDB. Sin embargo, un único MDR no suele detectar la existencia de otros MDR, ni se centra en las relaciones que un determinado CI pueda tener con otros CI (especialmente si están contenidos en otros MDR). CA CMDB está particularmente bien adaptado para gestionar este tipo de entornos debido a que se centra en la gestión de los CI independientemente de su fuente MDR.

El objetivo de CA CMDB no es almacenar todos los atributos de todos los CI, sino que se utiliza para consolidar los atributos más importantes que se deben gestionar de forma centralizada. Los atributos controlados por la gestión de cambios son excelentes candidatos para la inclusión en CMDB. El lanzador MDR permite acceder a los atributos que no están gestionados por CA CMDB. Además, CA CMDB proporciona el visor de CMDBf, que permite la comparación en paralelo de los atributos del CI específico entre varios CMDB y MDR.

Definición de MDR para CA Service Desk Manager

La ficha Administración le permite definir un MDR para CA CMDB.

Para poder importar cualquier CI a un MDR, es preciso que el MDR ya esté definido. Los intentos de importar un CI federado a un MDR inexistente fallarán.

Nota: Para obtener las instrucciones de definición de un MDR, consulte la *Guía de implementación*.

Lanzador MDR

El lanzador MDR es una herramienta de integración abierta que le permite ver los datos prácticamente desde cualquier MDR, utilizando una página Web sin utilizar ninguna codificación. El lanzador MDR permite a la persona que esté visualizando un CI obtener más información sobre dicho CI, así como obtener su control (si el MDR admite dicho control).

Entre los usos del lanzador MDR se incluyen los siguientes:

- En la página de detalles hardware.servidor, inicia CA Cohesion ACM para verificar un cambio.
- Desde la ventana de detalles de un CI de aire acondicionado, inicia la página Web de un proveedor para obtener información de diagnóstico e informes de incidentes.
- Desde un CI de contratos, inicia el sistema de gestión de contratos para conocer los detalles de los contratos.
- Desde un CI de SLA (Acuerdo de nivel de servicios), inicia el servicio de CA para revisar los acuerdos de nivel de servicios antes de realizar un cambio.
- Desde un CI de servidor, inicia el Control remoto de CA para utilizar el servidor para el diagnóstico y corrección de un problema.

Definición de una URL para iniciar un MDR

CA CMDB utiliza una URL para iniciar una sesión de página Web con el MDR de origen para que el lanzador MDR funcione. El usuario define la URL que usa CA CMDB.

Procedimiento para definir una URL para un MDR

1. Haga clic en la ficha Administración.
2. En el panel izquierdo, abra CA CMDB, árbol Gestión de MDR.
3. Haga clic en Lista de MDR.
Aparecerá la página Lista de repositorios de datos de gestión (MDR).
4. Haga clic en un MDR existente (o cree y guarde un nuevo MDR).
Aparecerá la página Definición del proveedor de MDR.
5. Haga clic en Editar.
Aparecerá la página Actualizar definición de MDR.
6. Rellene los siguientes parámetros:

Nombre de host

Especifica la dirección de red o el nombre de DNS del servidor Web que proporciona las páginas Web para el MDR.

Puerto

Especifica el número de puerto que utiliza el servidor Web del nombre de host.

Ruta

Especifica la ruta a la página Web, incluyendo la propia página.

Parámetros

Especifica los parámetros utilizados para identificar el CI deseado en el MDR. CA CMDB enviará esta información al MDR.

Userid

Especifica el ID de usuario (userid), si un ID de usuario común tiene permiso de acceso al MDR.

Secreto compartido

Especifica la información que se comparte entre CA CMDB y el MDR. Para los MDR de CA Cohesion, el valor especificado aquí debe coincidir con el valor especificado en el archivo de propiedades de CA Cohesion, para el valor com.cendura.security.oneclickauth.secret.

Espacio de nombre de CMDBf

Especifica el valor de federated_asset_id que se pasa a la consulta como un ID local. Para CA CMDB, el valor es http://cmdb.ca.com/r1.

CMDBf Timeout

(Opcional) Especifica el límite de tiempo para la consulta de punto final de CMDBf. El valor predeterminado es diez (10) segundos.

Punto final de CMDBf

Especifica el punto final del servicio de consulta para el MDR. Es necesario para el visor de CMDBf y la recuperación de datos actualizados de MDR. Si utiliza CA CMDB como un proveedor de MDR, el valor es
http://nombrehost_cmdb:puerto_cmdb/axis/services/QueryPort.

Guarde la definición.

La URL queda definida.

Nota: Además, la URL puede contener las variables de sustitución para adaptar más el CI al MDR. Si desea obtener más información, consulte la *Guía de implementación*.

Configuración de un proveedor MDR de CA APM

Puede configurar un MDR para que sea el proveedor de CA APM.

Procedimiento para configurar un proveedor MDR de CA APM

1. En la interfaz Web, inicie una sesión como administrador.
2. Seleccione la ficha Administración. En el explorador de Administración, seleccione CA CMDB, Gestión de MDR, Lista de MDR.
3. Haga clic en Crear nuevo para especificar el MDR de CA APM
Aparecerá la definición del proveedor MDR.
4. Introduzca la información siguiente sobre el proveedor MDR:
 - Nombre del botón: especifique APM o cualquier otro nombre de botón válido. Recomendamos utilizar un nombre de botón de APM.
 - Nombre de MDR: especifique APM para Unicenter Asset Portfolio Management r11.3.4 o ITAM para CA APM r12.5.
 - Clase MDR: especifique GLOBAL.
 - Nombre de host: especifica el nombre de servidor de CA APM utilizando la dirección de red o el nombre de DNS del servidor Web de CA APM.
 - URL para el inicio en contexto: especifica `http://{nombrehost}:{puerto}/{ruta}?{parámetros}` y no se debe cambiar.

El formulario del proveedor de MDR rellena automáticamente los valores de ruta de acceso y de parámetros con la información necesaria de inicio en contexto de CA APM.

5. Haga clic en Guardar.

El proveedor de MDR de CA APM queda establecido.

Nota: Para obtener más información sobre el lanzador MDR, consulte la *Guía de implementación*.

Inicio en contexto desde CA CMDB para CA APM

La función Lanzador de MDR de CA CMDB admite el inicio en contexto para CA APM cuando CA APM y CA CMDB comparten la misma MDB. La interfaz de usuario de CA CMDB incluye un botón para la función de inicio en contexto en la ficha Atributos del formulario de detalles de un elemento de configuración cuando el usuario crea una definición especial de proveedor de MDR de CA APM.

La definición de MDR de CA APM tiene todas las capacidades de un MDR tradicional. La característica de control de versiones de CA CMDB admite también el inicio en contexto directamente desde una entrada de registro de atributo asociada con cada cambio de CA APM.

Importante: A diferencia de otros MDR, el MDR de CA APM se asocia automáticamente a cada CI o Activo. La clase MDR de GLOBAL y el nombre MDR de APM se utilizan para identificar el MDR de Unicenter Asset Portfolio Management r11.3.4. La clase MDR de GLOBAL y el nombre MDR de ITAM se utilizan para identificar el MDR de CA APM r12.5. El uso del MDR de CA APM es plenamente compatible con otros MDR, incluso para el mismo CI.

Propiedades de CI que admiten la federación de MDR

Las propiedades del elemento de configuración (atributos) identifican los activos para fines de federación de MDR.

ID del activo federado

La gente se reconoce en diferentes organizaciones mediante distintos identificadores. Le pueden conocer por los identificadores siguientes:

- Un apodo exclusivo para sus amigos más cercanos
- El permiso de conducir (identificación exclusiva asociada con el usuario)
- Un ID nacional de servicio militar (por ejemplo, una tarjeta de reclutamiento)
- Un número de la seguridad social
- Un número de identificación fiscal nacional

Cada uno de estos identificadores exclusivos se refiere a usted; sin embargo, el identificador sólo es válido cuando se utiliza para describirle en el repositorio adecuado.

De igual forma, un CI puede tener varios identificadores para asociarlo con sus MDR de origen. Los CI son reconocidos por los MDR a través de un único identificador. Este identificador se denomina *ID del activo federado*. El proceso de asociar un CI con uno o varios MDR se denomina *asignación de CI*.

La asignación se produce cuando los CI se cargan en la MDB de una o dos formas:

- Definición de la asignación de CI mediante la interfaz de usuario de administración
- Carga de CI mediante la utilidad GRLoader

Nombre MDR

El nombre MDR se utiliza para identificar el MDR en CA CMDB cuando se exportan datos mediante XML y GRLoader. Normalmente, el MDR tiene su propia convención de nomenclatura para identificarse a sí mismo: una combinación del nombre de servidor host y el nombre o el número de una instancia identificadora. Como sólo existe un MDR en un host determinado, el nombre MDR se establece a menudo como nombre del servidor host.

Requerido para el visor de CMDBf

Importante: el nombre MDR de la versión 11.3.4 de Unicenter Asset Portfolio Management es APM y el nombre MDR para CA APM r12.5 es ITAM. Los dos productos son compatibles; sin embargo, se recomienda verificar la disponibilidad del producto en supportconnect.ca.com antes de implementarlos.

Clase MDR:

La clase MDR es definida por el cliente para agrupar MDR.

Nota: Se necesita una clase MDR de CMDBf para la visualización de CMDBf.

Importante: El nombre MDR y la clase MDR deben ser exclusivos en su empresa.

Definición de MDR con la instalación de CA Cohesion ACM

Los MDR de CA Cohesion ACM tienen los requisitos siguientes:

- El `mdr_name` especificado en la definición de MDR del servidor de CA CMDB debe coincidir exactamente con el valor del atributo `com.cendura.installation.name` del archivo `cendura.properties` del servidor de CA Cohesion ACM de destino.
- Los MDR de CA Cohesion ACM deben tener una clase MDR de Cohesion.
- El MDR debe especificar el nombre de host y el número de puerto del servidor de CA Cohesion ACM.

Para ejecutar el lanzador MDR, edite la parte siguiente del archivo `cendura.properties`:

```
# -- Configure One-Click Authentication --
com.cendura.security.oneclickauth.secret=shared_secret
com.cendura.security.oneclickauth.scheme=
com.cendura.security.oneclickauth.user=userid
```

Importante: El secreto que se ha especificado en el archivo `cendura.properties` debe coincidir con el *secreto compartido* en la definición de MDR.

El lanzador MDR inicia sesión con la *identificación del usuario* especificada en el archivo de propiedades y hereda sus atributos de seguridad. Para utilizar funciones como la actualización de atributos de CI, debe verificar que este usuario tiene suficientes privilegios.

Nota: Para obtener más información acerca de la creación de usuario y la configuración de las opciones de seguridad para ese usuario, así como acerca de la personalización del archivo de propiedades, consulte la *Guía de implementación de CA Cohesion ACM*.

MDR de CA Cohesion ACM

Los MDR de CA Cohesion ACM deben definirse antes de importar los datos de un servidor de CA Cohesion ACM. Un MDR de CA Cohesion ACM debe especificar una clase MDR de Cohesion.

Ejemplo: definición de MDR Cohesion1

En la definición siguiente de MDR Cohesion1, XML especifica un nombre MDR de cohesion_server y una clase MDR de Cohesion. Estos valores son necesarios para poder importar los CI.

Nombre del botón

Cohesion1

Nombre MDR

cohesion_server

Clase MDR:

Cohesion

¿Activo?

Activo

Propietario

CMDBAdmin

Descripción

El servidor de CA Cohesion ACM en Chicago

Nombre de host

cohesion_server

Puerto

8090

Ruta

CAisd/html/cmdb_cohesion.html

Parámetros

hostname={nombrehost}+port={puerto}+family={familia}+name={nombre}+secret={contraseña}+federated_asset_id={id_activo_federado}

ID de usuario

cohesion_userid

Secreto compartido

Chicago01

URL para el inicio en contexto

http://cmdb_hostname:8080/{ruta}?{parámetros}

Además, debido a que se trata de un servidor Cendura, los valores anteriores deben coincidir con los valores del archivo `cendura.properties` de dicho servidor, tal como se muestra en el siguiente ejemplo:

```
com.cendura.security.oneclickauth.secret=Chicago01
com.cendura.installation.name=cohesion_server
```

La sintaxis de la URL se puede modificar para gestionar requisitos especiales.

Cómo se asocia un MDR a un CI manualmente

Los MDR se pueden asociar manualmente con un CI mediante la utilidad de asignación de elementos de configuración federados que se encuentra en la ficha Administración de CA CMDB, en la rama Gestión de MDR del árbol.

Antes de asociar un CI a un MDR, realice lo siguiente:

1. Crear la definición de MDR (si todavía no existe).
2. Crear la definición de CI (si todavía no existe).
3. Identificar el ID del activo federado exclusivo del CI que desea conectar al MDR. Este ID es específico del MDR, por lo que se sale del ámbito de este documento.

Nota: Para identificar este ID de activo federado, consulte la documentación del MDR.

Importación automática de CA Cohesion

Es posible importar los CI directamente desde CA Cohesion ACM. Para ello es necesario ejecutar un informe de CA Cohesion ACM que especifique el nombre de host, el puerto, el ID de usuario y la contraseña de un servidor de CA CMDB. Si el MDR está definido en CA CMDB, CA Cohesion genera automáticamente el XML para crear los CI y las relaciones, junto con la información necesaria para ejecutar el lanzador MDR en un CI. El informe importa automáticamente los CI en CA CMDB.

Nota: Para obtener más información sobre la exportación de CI desde CA Cohesion ACM, consulte la ayuda en línea que está disponible en la ficha Informes, Plantillas de informes.

Asignación de un CI al MDR

Como cada MDR utiliza un `federated_asset_id` para identificar un CI, un CI puede estar relacionado con varios MDR. Un `federated_asset_id` no tiene que ser exclusivo en los distintos MDR, pero sí debe serlo dentro de un mismo MDR. Cada MDR debe tener una clase MDR y nombre MDR exclusivos.

Importante: Siempre que un CI o un proveedor MDR tengan un estado Inactivo, todas las asignaciones de CI federados asociadas con el CI o el proveedor MDR también tendrán el estado Inactivo.

Después de crear una definición del proveedor de datos de MDR, realice lo siguiente:

1. Crear un CI en CMDB que haga referencia a un MDR.
2. Comprobar que la definición de MDR funciona.

Como la ejecución sólo se puede iniciar desde el contexto de un CI, no es posible realizar la prueba directamente desde una definición de MDR que no tiene contexto de CI.

Puede ver la Lista de elementos de configuración federados en la ficha Administración, en el nodo Asignación de elementos de configuración federados.

Para ver el CI en un contexto MDR concreto, haga clic en el botón de ejecución de MDR.

El MDR de destino se inicia en el contexto del CI que ha sido abierto.

Ejemplo: Asignación de CI

1. Haga clic en la ficha Administración.
2. Desplácese a Gestión de MDR, Asignación de elementos de configuración federados.

Aparece la Lista de elementos de configuración federados.

3. Introduzca servidor1 en el campo Nombre de CI.

Las columnas siguientes muestran los valores:

ID del activo federado

1000234

1000235

Nombre CI

servidor1

servidor1

Proveedor MDR

Cohesion1

Cohesion2

Activo

Activo

Activo

El proveedor MDR de Cohesion1 conoce la existencia de servidor1, y el proveedor MDR de Cohesion2 también conoce la existencia de servidor1. El ejemplo siguiente muestra que cada uno de ellos ha asignado de forma independiente al servidor un identificador exclusivo.

4. Haga clic en el nombre de CI servidor1.

Aparecerá la página Detalles del elemento de configuración servidor1 que incluye botones de inicio con los nombres Cohesion1 y Cohesion2.

5. Haga clic en cualquier botón de inicio del proveedor MDR.

Aparecerá información adicional sobre el elemento de configuración.

Administración de definición de MDR

La administración de definiciones de MDR es un proceso flexible. Los parámetros de una definición de MDR se pueden modificar aun cuando los CI hagan referencia a ella. Por ejemplo, puede modificar el nombre del botón, nombre de host, ID de usuario, secreto compartido y otros después de haber definido el MDR y cargado los CI.

Informe de CA Cohesion ACM

CA Cohesion ACM proporciona una utilidad para programar informes recurrentes. Esta utilidad se puede usar para simplificar el proceso de mantener la CMDB sincronizada con los datos en el MDR de CA Cohesion ACM. Algunos errores comunes, como una contraseña no válida (debido a su cambio o vencimiento) pueden impedir que se importen los datos. Para conocer cualquier error que pudiera producirse durante la ejecución de los datos de fondo de la importación de datos, active la opción Notificación de Exportar informe de CA CMDB en CA Cohesion ACM. Recibirá un correo electrónico que le informa de cuándo se produce un error de importación. Si ejecuta el informe de Cohesion en segundo plano como una tarea programada, se recomienda activar la opción de notificación.

Nota: Para obtener información sobre la programación de la ejecución de la tarea Exportar informe de CA CMDB con regularidad, consulte la *Guía del producto CA Cohesion ACM*.

Importación de CI a CA CMDB mediante GRLoader

Al cargar un CI a CA CMDB mediante GRLoader, se deben rellenar los siguientes campos en XML para que el lanzador MDR funcione:

- <mdr_class>
- <mdr_name>
- <federated_asset_id>

Los valores especificados para <mdr_name> y <mdr_class> en XML deben coincidir exactamente con los valores proporcionados en la definición de MDR.

Importante: El nombre y la clase MDR se deben definir utilizando la interfaz de administración antes de importar los CI que hacen referencia al MDR. Si el MDR especificado en el XML no está definido, el CI no se importará.

Restricciones y convenciones de nomenclatura de los elementos de información

Los CI tienen las siguientes restricciones y convenciones de nomenclatura:

- Nombre CI

Se trata del nombre común o de visualización utilizado en todas las listas de CI. La longitud total del nombre no debe superar los 255 caracteres. El nombre de CI no necesita para ser exclusivo, pero recomendamos que sí sea globalmente exclusivo. Además, para aquellas situaciones en las que el nombre lo determina un MDR, se recomienda que los administradores de MDR acentúen la legibilidad humana al rellenar este campo.

- Elementos de configuración de software

En el caso de software de terceros, aplique la misma convención de nomenclatura a los CI que a los nombres que crea manualmente en la ficha Administración. La coincidencia de las convenciones de nomenclatura permite que los CI detectados de CA Cohesion ACM se concilien con los que se han creado manualmente. Si no se sigue esta convención, se pueden crear varios CI aun cuando sólo haya una instancia de software.

- Uso del atributo nombredesistema

El atributo nombredesistema asocia de forma exclusiva un *único* CI con un nombre de host concreto.

Si se importan varios CI que especifican el mismo nombredesistema que un CI existente, la conciliación ayuda a garantizar que sólo exista un único CI.

Ejemplo

Las líneas de salida siguientes muestran la creación de un CI de servidor (proveedor), un CI de software (dependiente), y una relación tipo *ejecuta* entre ellos. La relación resultante representa un servidor que ejecuta el software Apache.

```
CI: Nombre: Servidor1      Clase: Servidor  Nombredesistema: Servidor1
CI: Nombre: Apache1  Activado Servidor1      Clase: Software
Relación: Servidor1 ejecuta Apache1  Activado Servidor1
```

Convención de nomenclatura system_name

Recomendamos los siguientes estándares de nomenclatura para los CI de software y todos los MDR, para que otros MDR puedan integrarse bien con CA Cohesion ACM y entre sí, y para conciliar los CI correctamente. CA Cohesion ACM sigue estos mismos estándares.

System_name

Identifica de forma exclusiva los CI de software. Cuando se define una relación que implica un CI de software, especifica el mismo system_name que el de la definición de CI. Si se instalan varias instancias de la misma versión del mismo software en el directorio del mismo nombre de host, modifique system_name para imponer la exclusividad. La longitud total de system_name no debe superar los 255 caracteres. Si se infringe esta restricción, los datos pueden resultar dañados.

System_name debe ser un identificador exclusivo para esta instancia del software en un único host.

Utilice la siguiente sintaxis:

nombre de host | *nombre de software* | *versión* | *aplicación de empresa*

carácter de barra vertical (|)

Separa los varios campos en la concatenación de la sintaxis para permitir que el usuario utilice la facilidad de búsqueda.

nombre de host

Especifica el nombre de host que contiene el software.

nombre de software

Especifica un nombre común para el software.

version

Especifica el número de versión del software, si está disponible.

aplicación de empresa

Especifica un identificador exclusivo para esta instancia del software en *nombre de host*. Si la instancia del software está asociada con un servicio o aplicación de empresa, el nombre de dicho servicio es el calificador. Si no se puede determinar *aplicación de empresa*, es posible utilizar el directorio de instalación para identificar el software. Si la longitud total de este campo supera los 255 caracteres, utilice los puntos suspensivos (...) para que la longitud de este campo no sea superior a 255 caracteres.

Ejemplos: uso de la utilidad de búsqueda de la interfaz de usuario

Es posible usar la utilidad de búsqueda de la interfaz de usuario para buscar CI de software, como en los siguientes ejemplos:

Caso de uso	Nombre	System_name
Buscar todos los CI de software en el host	xxx	Xxx%
Buscar todas las instancias de software	yyy	yyy%
Buscar todas las instancias de software	yyy version 123.0	yyy% % % 123.0%

En la lista de resultados devuelta por la búsqueda anterior, el usuario sólo ve el campo Nombre.

```

mac_address      Null. - Inadecuado para el software
asset_num        Null  - Inadecuado para el software
serial_number    Null  - Inadecuado para el software
dns_name         Null  - Inadecuado para el software

```

Uso del Visor de CMDBf

CA Service Desk Manager proporciona el Visor de CMDBf para mostrar los resultados de la federación de elementos de configuración (CI) en los MDR. En una página de detalles de CI (o en el menú contextual del CI en la lista de elementos de configuración), haga clic en Visor de CMDBf para ver los atributos de CI de las CMDB y los MDR federados en paralelo. En la página Vista federada, puede hacer clic en Recuperar para actualizar la información de cualquiera de los MDR federados. Para facilitar la legibilidad, los archivos de metadatos de CA CMDB pueden conciliar los nombres de atributo de MDR con los de CA CMDB.

Nota: Esta opción requiere que los MDR admitan consultas. Puede configurar los puntos finales de CMDBf de MDR para que muestren sus resultados en Vista federada. Si desea obtener más información, consulte la *Guía de implementación*.

Si el elemento de configuración no tiene datos federados, el visor muestra solamente atributos de CA CMDB.

Cómo actualizar archivos de metadatos para la asignación de CMDBf

Para mejorar la lectura de las comparaciones de atributos, puede utilizar los archivos de metadatos de CA CMDB para traducir los nombres de atributo de MDR en nombres de atributo de CA CMDB. En cualquier atributo de MDR que no tiene una asignación de CA CMDB, la vista federada muestra el nombre de atributo enviado por el MDR. Los metadatos se pueden definir para que los proveedores de datos de CMDBf realicen lo siguiente::

- Mostrar valores de atributos de MDR mediante los nombres de atributo de CA CMDB
- Evitar que los atributos de proveedor de MDR se muestren en la vista federada
- Definir atributos de proveedor de MDR que no tienen equivalentes de CA CMDB

Los metadatos se definen con el archivo `cmdb_metadata_federation_viewer_site_attr.htmlpl`. Este archivo contiene las instrucciones sobre cómo actualizar el archivo. Los metadatos se puede aplicar a todas las familias de CMDB (atributos comunes) o a los atributos específicos de familias.

Para asignar nombres de atributo de MDR externos a las etiquetas de CA CMDB, se debe actualizar el formulario `cmdb_metadata_extensionable.htmlpl` respectivo, utilizando los siguientes campos en la macro `cmdbmetadata`:

- `mdr_attr`: nombre del atributo de MDR que se va a traducir.
- `mdr_name`: nombre del MDR que se traduce. Las expresiones regulares son compatibles.

Ejemplo: asignación de atributo

Las siguientes instrucciones de metadatos definen metadatos que comparan el atributo "phys_mem" de CA CMDB con el atributo de proveedor "mdr_memory" para todos los proveedores denominados "myMdr" o que comiencen con "MDR". Además, se compara "physical_memory" con "phys_mem" para todos los demás proveedores.

```
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="physical_memory"
provider_name_regexp=".*">
```

Ejemplo: ocultar un atributo

La siguiente instrucción de metadatos oculta el atributo "widget_cost" del proveedor de MDR a todos los proveedores denominados "myMdr".

```
<macro name=cmdbMetadata hide_provider_attr="YES"  
provider_attr="widget_cost" provider_name="myMdr">
```

Ejemplo: configuración de una etiqueta de atributo

La siguiente instrucción de metadatos define un nombre de atributo "ext_mem_capacity" que utiliza la etiqueta "Capacidad de memoria externa" en la categoría Atributos del visor de CMDBf.

```
<macro name=cmdbMetadata attr="ext_mem_capacity" category="Attributes"  
heading="Capacidad de memoria externa" help="Memoria externa total">
```

Más información:

[Cómo mostrar valores de atributo de MDR con nombres de atributo de CA CMDB](#) (en la página 635)

[Cómo ocultar atributos de proveedor de MDR](#) (en la página 636)

[Cómo definir atributos de MDR sin equivalentes de CA CMDB](#) (en la página 637)

[Definición de metadatos de proveedores de datos de CMDBf](#) (en la página 637)

Cómo mostrar valores de atributo de MDR con nombres de atributo de CA CMDB

Los metadatos puede crear una asociación entre los atributos del proveedor de MDR y los atributos de CA CMDB de manera que si se muestran juntos se pueden ver las diferencias y compartir las etiquetas. De forma predeterminada, los atributos de MDR que no tienen una asignación, se muestran en el visor como **No en CMDB**.

Los argumentos de la macro cmdbMetadata para comparar un atributo de CA CMDB con un atributo de proveedor de MDR incluyen:

- attr: nombre de atributo de CA CMDB
- provider_attr: nombre de atributo de proveedor de MDR
- provider_name: nombre de proveedor de MDR
- provider_name_regexp: expresión regular de nombre de proveedor de MDR

provider_name o provider_name_regexp son obligatorios.

Ejemplo: asociar los atributos de MDR con los nombres de atributo de CA CMDB

Las siguientes instrucciones de metadatos realizan las respectivas acciones:

- Comparar el atributo "phys_mem" de CA CMDB con el atributo de proveedor "mdr_memory" para todos los proveedores denominados "myMdr".
- Comparar el atributo "phys_mem" de CA CMDB con el atributo de proveedor "mdr_memory" para todos los nombres de proveedor que comienzan con "MDR".
- Comparar "physical_memory" con "phys_mem" para todos los demás proveedores.

```
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="physical_memory"
provider_name_regexp=".*">
```

Cómo ocultar atributos de proveedor de MDR

Algunos atributos de proveedor de MDR no deben mostrarse en la vista federada. Los metadatos de un proveedor de MDR se pueden ocultar para un proveedor de MDR determinado. Esta opción sólo se aplica a los atributos de proveedor de MDR y no se aplica a los atributos de CA CMDB.

Los argumentos de la macro cmdbMetadata para ocultar un atributo de proveedor incluyen:

- hide_provider_attr: "YES" oculta el atributo de proveedor de MDR
- provider_attr: nombre de atributo de proveedor de MDR
- provider_name: nombre de proveedor de MDR
- provider_name_regexp: expresión regular de nombre de proveedor de MDR

provider_name o provider_name_regexp son obligatorios.

Ejemplo: ocultar un atributo exclusivo de MDR

La siguiente instrucción de metadatos se puede utilizar para ocultar el atributo "widget_cost" del proveedor de MDR para todos los proveedores denominados "myMdr".

```
<macro name=cmdbMetadata hide_provider_attr="YES" provider_attr="widget_cost"
provider_name="myMdr">
```

Cómo definir atributos de MDR sin equivalentes de CA CMDB

Puede definir las etiquetas y el texto de ayuda para los atributos de proveedor de MDR que no se correspondan con ningún atributo de CA CMDB. En la vista federada, los atributos están etiquetados como No en familia.

Los argumentos de la macro `cmdbMetadata` para definir un atributo de proveedor incluyen:

- `attr`: nombre de atributo de CA CMDB
- `categoría`: nombre de la categoría en la que se muestra el atributo
- `encabezado`: etiqueta de encabezado para el atributo
- `ayuda`: descripción breve del atributo

Ejemplo: definir un atributo exclusivo de MDR

La siguiente instrucción de metadatos define un nombre de atributo `"ext_mem_capacity"` que utiliza la etiqueta "Capacidad de memoria externa" en la categoría Atributos de la vista federada.

```
<macro name=cmdbMetadata attr="ext_mem_capacity" category="Attributes"
heading=""Capacidad de memoria externa" help="Memoria externa total">
```

Definición de metadatos de proveedores de datos de CMDBf

Puede controlar el modo en que los datos se muestran en la vista federada.

Procedimiento para definir metadatos para el visor de CMDBf

1. Utilice Web Screen Painter para abrir el archivo `cmdb_metadata_federation_viewer_site_attr.htmlpl`.
2. Determine los cambios de metadatos que se necesitan.
Nota: En el archivo se ofrecen plantillas de ejemplo.
3. Copie la plantilla apropiada y sustituya por los argumentos requeridos de acuerdo con las instrucciones presentes en el archivo.
4. Guarde y publique los cambios.

Capítulo 16: Cómo gestionar el cambio

Esta sección contiene los siguientes temas:

[Gestión de Cambios de CA Service Desk Manager](#) (en la página 639)

[Componentes de gestión de cambios](#) (en la página 640)

[Visualización del calendario de cambios](#) (en la página 641)

[Responsabilidades de CAB](#) (en la página 642)

[Responsabilidades del gestor de cambios](#) (en la página 643)

[Definición de tareas para el rol del gestor de cambios](#) (en la página 644)

[Categorías de cambios, estado y niveles de riesgo](#) (en la página 645)

[Visualización del panel de resultados de órdenes de cambio](#) (en la página 646)

[Definición de consultas almacenadas de órdenes de cambio](#) (en la página 647)

[Configuración de las opciones del gestor de cambios](#) (en la página 648)

[Calendario de cambios](#) (en la página 649)

[Cómo programar órdenes de cambio](#) (en la página 662)

[Cómo programar ventanas para el cambio](#) (en la página 667)

[Detección de colisiones y análisis del conflicto](#) (en la página 671)

[Visualización de CA Workflow](#) (en la página 672)

[Definición de proceso de gestión de cambios para CA Workflow](#) (en la página 674)

[Generación de informes y Consola de CAB](#) (en la página 693)

[Evaluación de riesgos](#) (en la página 699)

[Explorador de impactos](#) (en la página 702)

Gestión de Cambios de CA Service Desk Manager

La gestión de cambios de CA Service Desk Manager es un conjunto de funciones para que los gestores de cambios, los coordinadores de cambios y los miembros del Comité de cambios (CAB) coordinen la revisión y la aprobación de las peticiones de cambio relativas a servicios y componentes de CI. Por ejemplo: los gestores de cambios pueden revisar y aprobar todos los cambios en servicios y componentes de elementos de configuración para garantizar que no se introduzcan nuevas vulnerabilidades de seguridad en el entorno de producción. El gestor de cambios dirige el CAB y es responsable de la aprobación de solicitudes de cambio en última instancia.

La Gestión de cambios incluye las siguientes funciones:

- Le permite seguir procesos de ITIL relativos a cambios de TI para la gestión de incidentes/problemas.

- Le permite ver información de gestión de servicios para un CI; por ejemplo, el número de cambios registrados en un CI, las fechas de implementación de los cambios y más.
- Le permite detectar colisiones cuando hay varias órdenes de cambio según las que se deben hacer cambios en los mismos CI al mismo tiempo.
- Le permite crear y almacenar ventanas para el cambio en el calendario de cambios.
- Le permite crear una orden de cambio en la vista de calendario.
- Le permite valorar los riesgos asociados con un cambio.

Nota: Para obtener información más detallada sobre cómo realizar los procedimientos de gestión de cambios, consulte la información sobre gestión de cambios de la *Ayuda en línea*.

Componentes de gestión de cambios

La gestión de cambios incluye los siguientes componentes:

Calendario de cambios

Muestra una vista gráfica de los eventos de cambio (see page 649), que incluye todas las peticiones de cambio programadas, en curso o con fallo, para CI y servicios en un vista de calendario (see page 662) configurable. El calendario también muestra fechas de desactivación, que son períodos de congelación. Los usuarios pueden crear una orden de cambio desde el menú contextual en las vistas diaria, semanal y mensual del calendario. El Gestor de cambios, los analistas de nivel 2 y los miembros de CAB utilizan esta función.

Programador de cambios

Muestra períodos de tiempo programados (see page 668) durante los cuales pueden producirse o no cambios en los CI en el calendario de cambios. El gestor de cambios utiliza esta opción para ver y crear asociaciones de CI y planificaciones de cambios durante el período de tiempo.

Detección de colisiones y análisis del conflicto

Analice las órdenes de cambio para ayudar a identificar posibles conflictos de implementación que podrían aumentar el riesgo de error. El Gestor de cambios utiliza esta función.

Visualización de workflow

Muestra el proceso de aprobación de solicitudes de cambios. El Gestor de cambios utiliza esta función.

Generación de informes y Consola de CAB

Muestra un panel de resultados (see page 693) que facilita la rápida aprobación en línea de órdenes de cambio que requieren la aprobación de CAB.

En CA Service Desk Manager, el Gestor de cambios puede generar un informe con detalles acerca de las solicitudes propuestas de cambios listos para su revisión por el CAB y distribuirlos electrónicamente a todos los miembros de CAB.

Nota: Los usuarios con los privilegios pertinentes pueden mostrar informes de conformidad, previsiones, tendencias y volumen predefinidos para la gestión de cambios en BusinessObjects InfoView con CA Business Intelligence.

Evaluación de riesgos

Ofrece la capacidad de adjuntar evaluaciones de riesgos para cada solicitud de cambios enviada. La opción Encuesta sobre riesgos le permite crear encuestas para evaluar los riesgos y asociarlas a categorías de cambios. La encuesta sobre riesgos incluye una serie de preguntas tipo test o para responder libremente.

Explorador de impactos

Muestra relaciones entre elementos de configuración adjuntados a una orden de cambio. Explorador de impactos se inicia desde la página Detalles de órdenes de cambio para facilitar el análisis de impactos (see page 702) a petición. El Gestor de cambios utiliza esta función.

Visualización del calendario de cambios

CA Service Desk Manager puede iniciar diversas opciones de gestión de cambios (en conformidad con los estándares de COBIT e ITIL) para ver o crear órdenes de cambio después de haber seleccionado un día en el *calendario de cambios*. Las nuevas órdenes de cambio se programan automáticamente para el día seleccionado.

El calendario de cambios informa conflictos, discordancias y posibles riesgos entre planificaciones de cambios, órdenes de cambio y CI. Puede utilizar el calendario para comprender los próximos cambios, su posible repercusión en el entorno de TI, etc.

Procedimiento para ver el Calendario de cambios

1. Haga clic en la ficha Calendario de cambios

Aparecen los campos del filtro del Calendario de cambios.

2. Rellene los campos de búsqueda para mostrar una vista de calendario que muestra la programación para las órdenes de cambio de interés.
3. Haga clic en Buscar.

El calendario de órdenes de cambio muestra la información que coincide con los criterios de búsqueda especificados.

Responsabilidades de CAB

El Comité de cambios (CAB) coordina la revisión y la aprobación o el rechazo de peticiones de cambio correspondientes a servicios y componentes de CI. Los miembros de CAB son responsables de lo siguiente:

- Revisar todos los cambios importantes en los sistemas de producción.
- Asistir a todas las reuniones pertinentes de CAB como requiera el Gestor de cambios.
- Revisar todas las solicitudes enviadas en relación con cambios para determinar su repercusión, los recursos necesarios para implementarlas y los costes permanentes.
- Participar en la programación y coordinación del Calendario de cambios.
- Ayudar a asegurar que se evalúen todos los cambios y se les dé la prioridad oportuna.
- Participar en las revisiones una vez que haya terminado la instalación.

Más información:

[Funcionamiento de procesos de CAB](#) (en la página 642)

Funcionamiento de procesos de CAB

El CAB es responsable de la revisión de todos los cambios importantes en sistemas de producción. Se notifica a los miembros de CAB que una solicitud de cambio requiere su aprobación, y estos realizan lo siguiente:

1. Listar las solicitudes de cambios que el CAB debe revisar.
2. Abrir la Consola de CAB y ver la información contenida en la solicitud.
3. Ver la justificación de negocio, el plan de implementación, los elementos de configuración y la documentación justificativa asociada a la solicitud y decidir si la aprueban o la rechazan.
4. Aprobar o rechazar la orden de cambio; la siguiente orden de cambio aparece automáticamente en la lista.

Se notifica automáticamente a la persona que solicita el cambio que el estado de CAB se ha actualizado con respecto a la solicitud de cambio.

Más información:

[Responsabilidades de CAB](#) (en la página 642)

Responsabilidades del gestor de cambios

El Gestor de cambios es responsable del proceso general de gestión de cambios empresariales y de la aprobación de órdenes de cambio en última instancia. También generan los informes de análisis de las medidas de gestión de cambios y hacen lo siguiente:

- Revisar las solicitudes de cambios y agregar a las partes interesadas y los aprobadores que sean precisos.
- Facilitar la resolución de incidencias, por ejemplo, detectando colisiones y conflictos de programación en el calendario.
- Revisar los planes de reserva y retroceso y la instalación para comprobar su accesibilidad y firmeza.
- Conocer el riesgo de cada cambio y garantizar que se asigne al cambio el nivel de riesgo apropiado.
- Controlar los cambios de sus respectivas áreas para garantizar que cumplan los requisitos de gestión de cambios de tecnología.
- Representar sus respectivas áreas y comunicar la repercusión de los cambios con un alto nivel de riesgo en la reunión semanal de CAB.
- Facilitar revisiones una vez que haya finalizado la instalación para detectar instalaciones problemáticas y cambios que no han funcionado.
- Servir como punto de escalación de solicitantes de cambios, de partes interesadas, de responsables de aprobación y de implementación y de grupos de apoyo.

Más información:

[Funcionamiento del rol del gestor de cambios](#) (en la página 643)

Funcionamiento del rol del gestor de cambios

El gestor de cambios es responsable de supervisar las órdenes de cambio para el entorno operativo con el fin de asegurar que los miembros del equipo de operaciones cumplen con los procesos y las políticas de negocio. El calendario de cambios puede facilitar la resolución de incidencias como conflictos de orden de cambio programando fechas de cancelación y periodos de inmovilización durante los cuales un CI o un conjunto de CI pueden cambiarse. Los gestores de cambio también realizan lo siguiente:

1. Supervisar la Consola de CAB, desde la cual se gestiona la rápida aprobación en línea de órdenes de cambio y solicitudes de cambios.
2. Organizar CAB con los miembros pertinentes para las órdenes de cambio que se están considerando y realizar reuniones regulares programadas de CAB para revisar las órdenes de cambio entrantes.
3. Crear informes con datos acerca de las solicitudes de cambios propuestas listos para su revisión por el CAB y distribuirlos electrónicamente a todos los miembros de CAB.
4. Realizar una revisión en tiempo real de cada solicitud de cambios y actualizar el registro con la decisión de CAB durante la reunión de éste.
5. Utilizar BusinessObjects InfoView para gestionar informes de cumplimiento, previsiones y tendencias y crear informes a petición.
6. Representar a sus respectivas áreas y comunicar la repercusión de los cambios con un alto nivel de riesgo en las reuniones de CAB.
7. Conocer el riesgo de cada cambio y garantizar que se asigne al cambio el nivel de riesgo apropiado.

Definición de tareas para el rol del gestor de cambios

Se pueden definir tareas para el rol del gestor de cambios

Procedimiento para definir tareas del rol del gestor de cambios

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Gestión de roles, Lista de roles.
Aparecerá la página Lista de roles.
2. Seleccione el rol Gestor de cambios.
Aparecerá la página Detalles del rol Gestor de cambios.
3. Haga clic en Editar.
Aparecerá la página Actualizar el rol Gestor de cambios.

4. Utilice las fichas y los campos siguientes para configurar las tareas y los permisos de acceso del rol Gestor de cambios:
 - Autorización
 - Acceso a función
 - Interfaz Web
 - Gestión del conocimiento
 - Visibilidad de documento de KT
 - Fichas
 - Formularios Web
 - Ir a Recursos
 - Acceso de lectura del cliente
 - Acceso de escritura del cliente
5. Haga clic en Guardar, Cerrar ventana.

Se actualiza el registro del rol Gestor de cambios.

Nota: Para obtener más información acerca de las fichas que aparecen en la página Detalles del rol Gestor de cambios, consulte la información sobre gestión de roles en la *Ayuda en línea*.

Categorías de cambios, estado y niveles de riesgo

Puede definir cómo funcionan las órdenes de cambio dentro de su entorno de servicio. Se pueden editar los valores predeterminados instalados con CA Service Desk Manager o definir unos propios.

Procedimiento para gestionar valores predeterminados de órdenes de cambio

1. Seleccione Service Desk, Órdenes de cambio en la ficha Administración.

2. Expanda el nodo Orden de cambio y seleccione *una* de las siguientes opciones:
 - Categorías
 - Tipos de cambio
 - Códigos de cierre
 - Estado del conflicto
 - Nivel de riesgo
 - Encuesta sobre riesgos
 - Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.
 - Código de estado de tarea de workflow
 - Tipos de tareas de workflowAparecerá la página Lista del elemento seleccionado.
3. Seleccione el elemento que desee editar.
Aparecerá la página Actualización de detalles.
4. Use los controles disponibles en las fichas de la parte inferior de la página para definir el funcionamiento de órdenes de cambio dentro de su entorno.
5. Haga clic en Guardar, Cerrar ventana.
Aparecerá el elemento actualizado en la lista.

Visualización del panel de resultados de órdenes de cambio

El panel de resultados de órdenes de cambio muestra las órdenes de cambio, los conflictos y las tareas programadas asignadas a analistas de nivel 2, gestores de cambios, coordinadores de cambios o miembros de CAB. Los usuarios pueden ver los registros asignados y no asignados por prioridad.

Procedimiento para ver el panel de resultados de órdenes de cambio

1. Desplácese a Órdenes de cambio en el panel de resultados de CA Service Desk Manager.
2. Expanda las carpetas para ver las carpetas anidadas relativas a lo siguiente:
 - Elementos abiertos y cerrados asignados o sin asignar.
 - Conflictos resueltos o sin resolver.
 - Las tareas programadas que comienzan hoy o la semana próxima.

3. Seleccione la carpeta correspondiente a los elementos que desea consultar.
Aparecerá la página Lista.
4. (Opcional) Haga clic en Mostrar filtro y rellene uno o varios campos para especificar los criterios de búsqueda que restringen la lista a los comentarios de interés.
5. Haga clic en Buscar.
La página Lista muestra los resúmenes de los elementos que coinciden con los criterios de búsqueda utilizados.
6. (Opcional) Haga clic en el botón Editar en lista para ver algunos campos más que pueden asociarse a un elemento.

Definición de consultas almacenadas de órdenes de cambio

La definición de consultas almacenadas que están a disposición de los usuarios en el panel de resultados de órdenes de cambio es una tarea administrativa. Existen dos opciones: modificar las consultas almacenadas instaladas incluidas con CA Service Desk Manager o definir unas propias.

Procedimiento para definir consultas almacenadas de órdenes de cambio

1. Seleccione Service Desk, Datos de aplicación, Consultas almacenadas en la ficha Administración.
Aparecerá la lista de consultas almacenadas.
2. Seleccione la consulta almacenada que desea editar.
Aparecerá la página Detalles de consulta almacenada.
3. Haga clic en Editar.
Aparecerá la página Actualizar consulta almacenada.
4. Edite los valores de campo según sea necesario.
5. Haga clic en Guardar, Cerrar ventana.
La consulta almacenada actualizada aparece en la lista de consultas almacenadas.

Ejemplo: Definición de una consulta almacenada para listar órdenes de cambio asignadas a un CAB al que pertenezca el usuario conectado

Este ejemplo demuestra cómo se puede crear una consulta almacenada que liste sólo órdenes de cambio asignadas a un CAB al que pertenezca el usuario conectado.

Procedimiento para crear la consulta almacenada

1. Desplácese al Panel de resultados de la página Actualizar consulta almacenada.
2. Edite los valores de los campos de la siguiente manera:
 - a. Seleccione el Uso de tablero.
 - b. Configure el tipo de orden de cambio.
 - c. Introduzca la cláusula Where:

```
cab.[group]group_list.member IN (@cnt.id) AND active = 1
```
3. Haga clic en Guardar, Cerrar ventana.
La consulta almacenada aparece en la lista de consultas almacenadas.

Más información:

[Generación de informes y Consola de CAB](#) (en la página 693)

Configuración de las opciones del gestor de cambios

Se pueden configurar opciones del rol Gestor de cambios

Procedimiento para configurar opciones del gestor de cambios

1. Seleccione Gestor de opciones en la ficha Administración.
2. Expanda el nodo Gestor de órdenes de cambio.
Aparecerá la lista de opciones.
3. Haga clic con el botón derecho en la opción que desee y seleccione Editar en el menú contextual.
Aparecerá la página Actualizar opciones.
4. Edite las opciones según sea necesario.
5. Haga clic en Guardar, Cerrar ventana.
La opción actualizada aparecerá en la lista de opciones.

Calendario de cambios

La opción *Calendario de cambios* ofrece una vista gráfica de los eventos de cambio con la hora de inicio y finalización de la implementación. Esta vista de planificación de cambios proporciona a los analistas y gestores una forma rápida de identificar cuándo se producen los eventos y cómo afectan al entorno, la organización y los recursos.

El calendario permite crear órdenes de cambio a partir de las vistas diaria, semanal y mensual, así como ver las ventanas de cambio global para las órdenes de cambio programadas. Si existen varias ventanas de cambio en un mes, se agrupan, por ejemplo, en un único grupo de ventanas de desactivación. Para ver los detalles de intervalos individuales, observe los detalles de una vista semanal o diaria o bien pase el ratón por encima para ver la información.

Más información:

[Cómo agregar información de programación a una orden de cambio](#) (en la página 649)

[Plantillas de eventos de iCalendar](#) (en la página 650)

[Exportación de programaciones a iCalendar](#) (en la página 651)

[Vistas de programación](#) (en la página 652)

[Programación de la configuración de vista](#) (en la página 654)

Cómo agregar información de programación a una orden de cambio

Al crear o editar una orden de cambio, se puede agregar información de programación.

Procedimiento para agregar información de programación

1. Realice una de las siguientes acciones:

- Seleccione Archivo, Nueva orden de cambio.
- Abra una orden de cambio y haga clic en Editar.

2. Rellene los siguientes campos de programación:

Tipo

Especifica el tipo de cambio ITIL como Estándar, Normal o Emergencia. Es posible que se defina un valor predeterminado para una categoría de cambio que CA Service Desk Manager utiliza a la hora de inicializar nuevas órdenes de cambio para la categoría.

Fecha de inicio de la programación

Especifica la fecha de inicio de la orden de cambio.

Duración

Especifica la duración de la orden de cambio en formato 00:00:00.

La programación contiene solamente las órdenes de cambio en las que la duración y la fecha de inicio de la programación no están vacías. El campo Tipo resulta útil para agrupar órdenes de cambio de la programación sin afectar directamente la programación.

3. Continúe creando la orden de cambio.
4. Al terminar, haga clic en Guardar.

La información de programación se agrega a la orden de cambio.

Plantillas de eventos de iCalendar

Las plantillas de eventos de iCalendar controlan la información que se exporta al formato iCalendar.

Las plantillas predefinidas siguientes se instalan con <USK>:

- Planificación de cambios
- KnowledgeScheduleCreation
- KnowledgeScheduleExpired
- KnowledgeScheduleReview
- KnowledgeScheduleStart

Nota: Puede editar los códigos predefinidos de la plantilla de eventos de iCalendar, pero no puede suprimirlos ni crear unos nuevos.

Importante: la variable SchedExpMaximum en web.cfg controla el número máximo de eventos permitidos para una exportación. Aumentar el valor predeterminado (1000) podría causar inestabilidad del sistema. Si intenta exportar más que el valor especificado en SchedExpMaximum, aparecerá un mensaje en el que se rechaza la solicitud de exportación.

Exportación de programaciones a iCalendar

El formato iCalendar es un estándar del sector para el intercambio de datos que permite importar las programaciones de orden de cambio a diversas aplicaciones de creación de calendarios ampliamente utilizadas, entre las que se incluyen Microsoft Outlook y Lotus Notes.

Nota: Si se selecciona la opción Abrir en lugar de Guardar durante la exportación de programaciones en algunos programas de creación de calendarios, el archivo no se importa correctamente. Para evitar esta incidencia en las programaciones de la gestión de conocimiento y de órdenes de cambio, seleccione la opción Guardar en lugar de Abrir. Después de guardar el archivo exportado, impórtelo a través de la interfaz del programa de creación de calendarios.

Importante: los datos que se exportan se basan en la vista actual. Si desea exportar un intervalo de fechas personalizado, como un intervalo de 32 días, la exportación se debe realizar desde la vista de lista. De lo contrario, la vista se trunca en un mes o una semana y se exporta solamente esa cantidad.

Procedimiento para mostrar el Calendario de cambios

1. Haga clic en la ficha Calendario de cambios
Aparecen los campos del filtro del Calendario de cambios.
2. Rellene los campos de búsqueda para ver una vista de lista o calendario que incluya las órdenes de cambio de interés.
3. Haga clic en Exportar.
Aparecerá la página Programar exportación.

Importante: la variable SchedExpMaximum en web.cfg controla el número máximo de eventos permitidos para una exportación. Aumentar el valor predeterminado (1000) podría causar inestabilidad del sistema. Si intenta exportar más que el valor especificado en SchedExpMaximum, aparecerá un mensaje en el que se rechaza la solicitud de exportación.

4. Introduzca la ubicación en la que desea guardar un archivo iCalendar.
Se guarda en la ubicación especificada un archivo iCalendar que contiene todos los eventos de la vista actual.

Vistas de programación

CA Service Desk Manager proporciona las siguientes vistas de programación:

Lista

Muestra una página de lista ordenada según las fechas de inicio y finalización de la programación.

Mes

Muestra un calendario para un mes completo.

La vista muestra las órdenes de cambio en grupos, con una entrada destinada a una o varias órdenes de cambio. Para ver información detallada sobre las órdenes de cambio de un grupo, coloque el puntero del ratón sobre el grupo; pulse Alt+Flecha derecha cuando el foco esté sobre el grupo; o haga clic en el grupo para ver su contenido en una vista de día n.

Semana

Muestra una semana completa en una sola columna que comienza con el día configurado como el primer día laborable.

La vista muestra los cambios en forma individual e incluye información detallada sobre cada orden de cambio programada para la semana.

Día

Muestra las órdenes de cambio para un solo día.

La vista muestra los cambios en forma individual e incluye información detallada sobre cada orden de cambio programada para el día.

n días

Muestra las órdenes de cambio del número de días especificado con el selector desplegable.

La vista muestra los cambios en forma individual e incluye información detallada sobre cada orden de cambio programada para los días seleccionados.

Navegación en las vistas de programación

Puede utilizar la tecla de tabulación o las teclas de flecha para navegar por las vistas de programación. Se encuentran disponibles los siguientes accesos directos:

Tab

Permite ir a una fecha posterior. Utilice esta opción en la última celda de la programación para ir al botón Buscar.

Mayús+Tabulador

Permite ir a una fecha anterior. Utilice esta opción en la primera celda de la programación para ir al botón Mes siguiente.

Tecla de mayúsculas+Tecla de flecha

Permite navegar por el calendario de fecha en fecha en la dirección que indica la flecha.

Flecha derecha

Muestra el menú contextual de la fecha o el evento que se encuentra enfocado en ese momento. Si no hay un menú contextual, permite ir a la siguiente fecha más alta (similar a Tecla de mayúsculas+Flecha derecha).

Alt+Flecha derecha

Muestra un mensaje emergente que aparece al pasar el puntero del ratón sobre una fecha o un evento y ofrece información de la fecha o el evento enfocado en ese momento. Si no existe ningún tipo de información para mostrar al pasar el puntero, permite ir a la siguiente fecha más alta (similar a Tecla de mayúsculas+Flecha derecha).

Flecha abajo

Permite ir al siguiente evento de la celda actual. Si no hay ningún evento en la celda actual, o si el foco ya se encuentra en el último evento, permite ir a la fecha de la siguiente celda hacia abajo (similar a Tecla de mayúsculas+Flecha abajo).

Flecha arriba

Permite ir al evento anterior de la celda actual. Si el foco no se encuentra en un evento, permite ir a la fecha de la siguiente celda hacia arriba (similar a Tecla de mayúsculas+Flecha arriba).

Tecclas de acceso rápido de la vista de calendario

Cada vista de programación admite teclas de acceso rápido para sus botones. A continuación se presentan las teclas de acceso rápido admitidas:

Alt+0

Permite pasar a la vista de lista.

Alt+1

Permite pasar a la vista diaria.

Alt+7

Permite pasar a la vista semanal.

Alt+3

Permite pasar a la vista mensual.

Alt+9

Permite pasar a la vista de día *n*.

Alt+<

Permite ir al periodo anterior de la vista actual.

Alt+>

Permite ir al siguiente periodo de la vista actual.

Programación de la configuración de vista

Para configurar las vistas de programación mensual y semanal, especifique las declaraciones `pdm_macro` en la sección `<head>` de los formularios HTML que definen la programación. Se recomienda utilizar la vista de fuente de Web Screen Painter para modificar estos formularios.

Todos los formularios que muestran una programación deben incluir lo siguiente:

- Una macro `schedConfig`
- Una macro `schedAttr`, como mínimo
- Una macro `schedGroup`, como mínimo

Las macros de configuración se ubican en un archivo de origen separado al cual hace referencia la declaración `pdm_include` en un archivo de origen principal. Este archivo permite configurar la programación sin modificar el archivo de origen principal.

Por ejemplo, las macros de configuración para el formulario de calendario de cambios `list_chgsched.html` se encuentran en un archivo denominado `list_chgsched_config.html`. En la programación de ciclo de vida de conocimientos se puede modificar el archivo `list_kdsched_config.html` que utiliza las mismas macros.

Los archivos `list_chgsched_config.html` y `list_kdsched_config.html` se encuentran en el siguiente directorio:

`$NX_ROOT\bopcfg\www\html\web\analyst\`

Macro `schedConfig`: configurar programación

La macro `schedConfig` indica que un formulario contiene una programación y proporciona información de configuración básica. Los siguientes valores son argumentos de macro válidos:

`autosearch=1|0`

Especifica si el formulario de programación vuelve a cargar los datos del servidor cuando el usuario selecciona una vista fuera del intervalo de fechas actualmente seleccionado. Al establecer el valor en 1 (opción predeterminada), cuando el usuario selecciona una vista con uno o más días fuera del intervalo de selección de datos del filtro de búsqueda, el formulario realiza la búsqueda en forma automática. Al establecer el valor en 0, el usuario debe hacer clic en el botón **Buscar** para iniciar una búsqueda.

`defaultView=0|1|7|30|99`

Especifica la vista predeterminada para el filtro de búsqueda como 0 (lista), 1 (día), 7 (semana), 30 (mes) o 99 (día n).

La especificación de `defaultView` afecta solamente a la visualización inicial del filtro de búsqueda. Una vez que se muestra la programación, CA Service Desk Manager mantiene automáticamente la selección de la vista de filtro alineada con la vista actual.

Valor predeterminado: 30

`firstday=0|1|2|3|4|5|6|7`

Especifica el primer día laborable de la vista mensual como un número entre 0 (domingo) y seis (sábado).

Valor predeterminado: 0

export=xxx|0

Especifica el nombre del código de la plantilla utilizada para realizar la exportación en el formato iCalendar. Al establecer el valor en 0, la función de exportación y el botón Exportar quedan deshabilitados.

Valor predeterminado: ChangeSchedule

legend=1|2|0

Especifica la ubicación de la leyenda de la programación que muestra el nombre y el formato de los grupos de la programación. Puede establecer el valor en 1 para ubicar la leyenda por encima de la programación o en 2 para ubicar la leyenda por debajo de la programación. Puede establecer el valor en 0 para deshabilitar la leyenda.

Valor predeterminado: 2

maxGroups=0/n

Especifica el número máximo de grupos que se pueden mostrar en una sola celda de la vista mensual de calendario.

Si el número en el valor maxGroups programado para un solo día supera el máximo, CA Service Desk Manager muestra solamente el primer valor maxGroups-1 y reemplaza el último con un hipervínculo "..nn más cambios" sobre el cual el usuario puede pasar el ratón o hacer clic para ver la lista completa. Puede establecer el valor en 0 para deshabilitar esta función y permitir un número ilimitado de eventos en una celda del calendario.

Valor predeterminado: 4

nday=(n,n ...)

Especifica selecciones para la lista desplegable de la vista de día n.

La especificación es una lista de recuentos de los días que se van a incluir en la lista desplegable. El valor 0 se utiliza para indicar que la lista desplegable de día n se omite de la programación. El primer valor especificado es el valor predeterminado para la lista desplegable.

Valor predeterminado: (3,7,14,28)

round=(hr,min)|0

Especifica si las fechas de inicio y finalización de la programación se deben redondear al recopilar órdenes de cambio o documentos de conocimiento en grupos. Especifique round=0 para deshabilitar el redondeo.

De forma predeterminada, las fechas de inicio y finalización de la programación agrupan objetos. Todas las fechas de CA Service Desk Manager incluyen una hora, sin redondear, y los objetos programados a tan solo un minuto de diferencia se ubican en grupos separados. El redondeo determina el grupo después de ajustar la fecha de inicio a una hora o un minuto más temprano y la fecha de finalización a una hora o un minuto más tarde.

El valor de redondeo especifica una hora o un minuto (pero no ambos). Las horas se redondean al múltiplo más cercano del valor especificado, por ejemplo:

round=(0,15)	redondea al cuarto de hora más cercano
round=(0,30)	redondea a la media hora más cercana
round=1	redondea a la hora más cercana
round=12	redondea al medio día más cercano (0:00 ó 12:00)
round=24	redondea al día más cercano

Valor predeterminado: (0,15)

timefmt=24hr|([am],[pm])

Especifica el formato de las horas en las vistas de calendario de la programación.

El valor predeterminado 24hr indica que las horas se muestran en un formato de 24 horas (0:01 a 23:59). El valor alternativo (am,pm) especifica un sufijo para las horas de la mañana o de la tarde, o ambas.

Nota: Todos los argumentos schedConfig son opcionales.

Macro schedAttr: especificar un atributo almacenado

La macro schedAttr especifica un atributo almacenado para cada elemento que se selecciona de la lista. Los atributos almacenados están disponibles en la información que aparece al pasar el ratón por encima de la vista mensual, en la información detallada o de resumen de todas las vistas excepto la mensual y en la función setSchedEvents() de JavaScript. Los siguientes valores son argumentos de macro válidos:

attr=xxxx

(Obligatorio) Especifica un atributo de un objeto de la programación, como una orden de cambio o un documento de conocimiento. Se permiten atributos con puntos. El nombre de atributo de palabra clave CInn puede utilizarse en el calendario de cambios para especificar que las primeras nn clases asociadas con la orden de cambio están incluidas en la información almacenada.

Nota: Este argumento es el único argumento obligatorio de la macro schedAttr.

attrRef=.COMMON_NAME|xxxx

Almacena el atributo de la tabla almacenada para un atributo SREL (ignorado para los atributos que no sean SREL) a la que se hace referencia. El nombre del atributo especificado debe incluir un punto como prefijo.

Valor predeterminado: .COMMON_NAME

label=

Muestra una etiqueta para el atributo de la vista de día n.

Valor predeterminado: DISPLAY_NAME en Majic del atributo

ident=1|0

Especifica si el atributo es un identificador del objeto (como el número de referencia de una orden de cambio). Los atributos que funcionan como identificadores se muestran sin etiquetas delante del nombre de grupo en la información que aparece al pasar el ratón y en la vista de día n.

Valor predeterminado: 0

detail=1|0

Especifica si el atributo se incluye en la información de detalle que se muestra en vistas que no sean la vista mensual. La información de detalle es la que se muestra cuando la casilla de verificación Sólo resumen no está activada en la vista.

Valor predeterminado: 1

hoverInfo=1|0

Especifica si el atributo está incluido en el cuadro emergente con información que aparece en la vista mensual al pasar el puntero del ratón por encima de un grupo, o cuando el usuario pulsa las teclas Alt+Flecha derecha y el foco se encuentra sobre el grupo.

Valor predeterminado: 0

summary=1|0

Especifica si el atributo se incluye en la información de detalle que se muestra en vistas que no sean la vista mensual. La información de detalle es la que se muestra cuando la casilla de verificación Sólo resumen no está activada en la vista.

Valor predeterminado: 0

Nota: CA Service Desk Manager muestra los atributos en la información de resumen, la información detallada o la información que aparece al pasar el ratón en el mismo orden que muestra sus macros schedAttr.

Macro schedGroup: especificar un grupo de eventos

La macro schedGroup especifica la codificación de nombre y color de un grupo de elementos. La vista mensual reúne todos los elementos en un grupo dentro de un solo evento. Todas las vistas excepto la mensual muestran los elementos en forma individual en el formato del grupo al cual pertenecen. Los siguientes valores opcionales son argumentos de macro válidos:

grpname=xxx

(Obligatorio) Especifica el nombre del grupo. La macro automáticamente asigna un número al grupo y asigna el número a una variable de JavaScript con el nombre del formulario schedGroup_xxx, en el que xxx es el nombre del grupo. Esta variable se puede utilizar en la función setSchedEvents() de JavaScript para crear un evento que pertenezca al grupo.

Nota: Este argumento es el único argumento obligatorio de la macro schedGroup.

label=xxx

Especifica una etiqueta para el grupo. Si se especifica una etiqueta, ésta se muestra en todas las vistas.

legend=xxx|0

Muestra una descripción del grupo para la leyenda que aparece en la parte inferior de la programación. Los grupos aparecen en la leyenda si por lo menos un ejemplo del grupo existe en la vista actual. Si se especifica 0, el grupo se excluye de la leyenda.

Valor predeterminado: 0

color=black|color

Especifica el color del texto de los elementos de este grupo. Puede especificar el color en formato CSS, un color Web válido o un valor hexadecimal precedido por un signo de número.

Ejemplo: Introduzca "#FF0000" o "red" para rojo.

Valor predeterminado: negro

bgcolor=white|color

Especifica el color de fondo de los elementos de este grupo. Puede especificar el color de fondo en formato CSS, un color Web válido o un valor hexadecimal precedido por un signo numeral.

Ejemplo: Introduzca "#FF0000" o "red" para rojo.

Predeterminado: blanco.

style=normal|bold|italic

Especifica el estilo de texto de este grupo como normal, negrita o cursiva.

Valor predeterminado: normal

Configuración de ventanas de mantenimiento y desactivación en el calendario de cambios

Se editan las instrucciones PDM_MACRO de `list_chgsched_config.html` para modificar los colores, las etiquetas, las leyendas y los iconos de las ventanas para el cambio.

Nota: Si utiliza macros `schedGroup` para cambiar el formato de ventanas en el calendario de cambios, también debe actualizar `schedule.css` si desea que el formato sea coherente con el planificador de cambios.

Procedimiento para configurar ventanas para el cambio

1. Abra el formulario `list_chgsched_config.html` en un editor de texto o en WSP.

Puede localizar este archivo en el directorio siguiente:

```
$NX_ROOT\bopcfg\www\html\web\analyst\
```

2. En la macro `schedGroup`, modifique las instrucciones PDM_MACRO siguientes:

Para ventanas de mantenimiento:

```
<PDM_MACRO NAME=schedGroup grpname=maintwindow  
  bgcolor=lightgreen  
  label="Maintenance"  
  legend="Maintenance window"  
  icon= "confirmation_12.png">
```

Para ventanas de desactivación:

```
<PDM_MACRO NAME=schedGroup grpname=blackoutwindow style=italic color=white  
  bgcolor=black  
  label="Blackout"  
  legend="Blackout window"  
  icon= "warning_12.png">
```

bgcolor

Especifica el color de fondo de la ventana.

etiqueta

Especifica la etiqueta de la ventana como Mantenimiento o Desactivación.

leyenda

Especifica el texto de la leyenda tal y como aparece en el calendario de cambios.

icon

Especifica una URL opcional de un gráfico web de 12x12 píxeles.

Este icono aparece con una orden de cambio o grupo en el calendario de cambios si la orden de cambio coincide por completo con una ventana de mantenimiento o se superpone a una ventana de desactivación.

3. Guarde el formulario.

Quedarán configuradas las ventanas para el cambio.

La función setSchedEvents() JavaScript

La función setSchedEvents() de JavaScript permite crear eventos en la programación. Modifique esta función cuando desee ver los objetos de cualquier grupo nuevo. Los objetos del grupo predefinidos aparecen de forma predeterminada.

CA Service Desk Manager invoca a la función setSchedEvents() una vez en relación con cada objeto (orden de cambio o documento de conocimiento) seleccionado por el filtro de búsqueda de la programación. Con el fin de crear eventos para el objeto, la función invoca a una segunda función, schedEvent(); y transfiere el ID de grupo, la fecha de inicio y la fecha de finalización del evento.

La función puede crear cualquier número de eventos (incluido cero) para un objeto. La función setSchedEvents() predeterminada para el calendario de cambios (list_chgsched.html) crea un evento para cada orden de cambio y agrupa estas órdenes por tipo de cambio. Esta función se codifica de la siguiente manera:

```

1.     función setschedEvents( chg )
2.     {
3.     var grpnum;
4.     switch( chg["chgtype"] - 0) {
5.         caso 100: grpnum = schedGroup_std; break;
6.         caso 300: grpnum = schedGroup_std; break;
7.         predeterminado: grpnum = schedGroup_norm; break;
8.     }
9.     chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"]);
10.    }
```

El parámetro de caso especifica el ID del tipo de cambio. Para conocer cómo se enumeran los ID de caso, consulte Creación de un tipo de cambio.

La función tiene un solo argumento perteneciente a un objeto de JavaScript que contiene los atributos que las macros schedAttr han especificado. La instrucción switch de las líneas 4-8 examina el atributo chgtype de la orden de cambio y asigna el número de grupo pertinente de una de las variables

schedGroup_xxxx definidas por las macros schedGroup anteriores. En la línea 9, la instrucción invoca a la función schedEvent() para crear un evento en la programación mediante la transferencia del número de grupo previamente asignado y de las fechas de inicio y finalización de la programación. Las fechas están disponibles en el objeto del argumento, ya que se especificaron en las macros schedAttr anteriores.

Cómo programar órdenes de cambio

Se puede ver la programación de todos los elementos de configuración asociados a una orden de cambio. Tenga en cuenta la información de programación cuando cree, edite o vea una orden de cambio, o cuando actualice el calendario de cambios. La visualización de la programación le puede ayudar a evitar las colisiones de programación.

Para ver y actualizar una programación, haga lo siguiente:

1. Cree o abra una orden de cambio.
2. Asocie elementos de configuración a la misma.

Nota: Si no asocia ningún elemento de configuración a la orden de cambio, aparecerá un error al hacer clic en el botón Programador.

3. Haga clic en Ver planificador.

Aparecerá el planificador de cambios y mostrará las vistas siguientes:

Diario

(Valor predeterminado) Muestra el período de tiempo de la orden de cambio en la fecha y hora seleccionadas. Si no se asocia ninguna fecha a la orden de cambio, la vista será de forma predeterminada la del día actual.

Semanal

Muestra el plazo de la orden de cambio en la semana actual e incluye la fecha de comienzo de la implementación, que se puede configurar para que sea la fecha de comienzo del calendario de cambios.

Nota: La duración de la programación determina la duración del sombreado en la programación. Por ejemplo, si crea una orden de cambio con dos horas de duración, aparecerá el sombreado en amarillo claro del programador durante las dos horas de duración definidas.

4. (Opcional) Haga clic en un elemento de configuración para ver los detalles. Coloque el puntero sobre el nombre del elemento de configuración para ver el nombre completo.
5. (Opcional) Modifique la fecha de inicio de la implementación o la duración.
 - a. Haga clic en Ver programación para obtener una vista previa de la programación actualizada.

b. Haga clic en Actualizar programación para actualizar la programación.

Nota: Sólo se puede modificar la programación en el modo de edición.

6. Guarde la solicitud de cambio.
7. Actualice el calendario de cambios para ver ventanas de cambio globales y asociadas a CI.

Uso del ejemplo del programador de cambios

El ejemplo siguiente demuestra cómo utilizar el programador de cambios al crear una orden de cambio.

1. En la ficha Service Desk, seleccione Archivo, Nueva orden de cambio.
Aparecerá la página Crear nueva orden de cambio.
2. Seleccione Actualizar elementos de configuración en la ficha Elementos de configuración.
Aparecerá la página Búsqueda de elementos de configuración.
3. Cree o busque CI.
4. Desde la página Actualizar elementos de configuración afectados, agregue CI a la orden de cambio.
5. Haga clic en OK.
Se actualizará la página Crear nueva orden de cambio.
6. Haga clic en el botón Programador.
Aparecerá la página Programación para orden de cambio.
7. Seleccione una vista y realice *cualquiera* de las siguientes acciones:
 - Haga clic dentro de las celdas de la tabla para modificar la Fecha de inicio de programación.
 - Haga clic en la Fecha de inicio de programación para utilizar el Asistente de fecha.
8. Modifique la Duración y haga clic en Ver programación.
La programación obtiene una vista previa de los cambios.
9. Haga clic en Actualizar programación.
La programación se actualiza con los cambios.
10. Guarde la solicitud de cambio.

Establecimiento de un número máximo de elementos de configuración

Se puede establecer el número máximo de elementos de configuración que aparecen en el programador de cambios.

Procedimiento para establecer el número máximo de elementos de configuración

1. Abra *NX.env*.

Puede localizar este archivo en el directorio siguiente:

`$NX_ROOT\`

2. Cambie el valor de `@NX_CHANGE_SCHEDULER_MAX_CI_CNT` por el número máximo que desee.

Nota: De forma predeterminada, la variable está establecido en 100. Si define como número máximo de elementos de configuración un valor superior a 100, sólo aparecerán los primeros 100 y se recibirá una advertencia.

3. Guarde *NX.env* y reinicie CA Service Desk Manager.

Queda establecido el número máximo de elementos de configuración.

Ejemplo: Establecimiento del número máximo de elementos de configuración en 25

En el ejemplo siguiente, sólo aparecen los primeros 25 CI en el planificador de cambios.

```
@NX_CHANGE_SCHEDULER_MAX_CI_CNT=25
```


Modificación del color de fondo de la duración de órdenes de cambio

Puede cambiar el color de fondo de la duración de órdenes de cambio. Modifique las líneas siguientes de *schedule.css* para cambiar el resaltado de la barra verde de duración de órdenes de cambio.

Procedimiento para cambiar el color de fondo

1. Abra *schedule.css*.

Puede localizar este archivo en el directorio siguiente:

```
$NX_ROOT\bopcfg\www\wwwroot\css
```

Importante: *\$NX_ROOT\sdk* también contiene un archivo llamado *schedule.css* que contiene comentarios útiles acerca de controles *css*.

2. Modifique las líneas siguientes con el código de color que desee:

```
td.noBorderBackColor{border-left:none;border-right:none;background-  
color:#F6E3CE;}  
td.withBorderBackColor{border-right:none;border-left:1px solid;background-  
color:#F6E3CE;}
```

3. Guarde *schedule.css*.

En el ejemplo siguiente, el color de fondo de la duración del cambio es #FF0000.

Ejemplo: Modificación del color de fondo de la duración del cambio a #FF0000

```
td.noBorderBackColor{border-left:none;border-right:none;background-  
color:#FF0000;}  
td.withBorderBackColor{border-right:none;border-left:1px solid;background-  
color:#FF0000;}
```

Cómo modificar los colores de las ventanas para el cambio en el planificador de cambios

Se pueden cambiar los colores que indican ventanas para el cambio modificando líneas de *schedule.css*.

Nota: Si modifica *schedule.css* para cambiar el formato de las ventanas en el planificador de cambios, también debe modificar las macros schedGroup utilizadas por el calendario de cambios si desea que el formato sea coherente con el planificador.

Procedimiento para cambiar el color de fondo

1. Abra *schedule.css* en un editor de texto.

Puede localizar este archivo en el directorio siguiente:

```
$NX_ROOT\bopcfg\www\wwwroot\css
```

2. Modifique las líneas siguientes con el código de color que desee:

```
.schedConflict { background-color: #ff0000; font-size: 4px; }  
.schedBusy { background-color: #0176ff; font-size: 4px; }  
.schedCurrent { background-color: #008000; font-size: 4px; }  
.schedMW { background-color: #40ff40; font-size: 4px; }  
.schedBW { background-color: black; font-size: 4px; }  
.schedNone {font-size: 4px; }  
.schedDialog { width: 100%; height: 4px; margin-left: 0px; margin-right: 0px;  
margin-top: 4px; margin-bottom: 4px; }
```

3. Guarde *schedule.css*.

Se modificará el color de fondo.

Más información:

[Macro schedConfig: configurar programación](#) (en la página 655)

Cómo programar ventanas para el cambio

Puede programar ventanas para el cambio y verlas en el Calendario de cambios. Las *ventanas de mantenimiento* establecen los períodos de tiempo en que deberían producirse los cambios de CI. Las *ventanas de desactivación* establecen los períodos de tiempo en que *no* deberían producirse los cambios de CI. Las ventanas para el cambio ayudan a programar los cambios para reducir al mínimo su impacto en los procesos importantes de negocio. CA Service Desk Manager puede implementar ventanas para el cambio en el nivel global o de sistema.

Para programar ventanas para el cambio, realice lo siguiente:

1. Vea el Calendario de cambios para determinar dónde desea las ventanas para el cambio.
2. Cree las ventanas para el cambio adecuadas para la organización.

ventana de mantenimiento

Indica un período de tiempo programado durante el cual se puede cambiar un elemento de configuración o un conjunto de éstos. Dado que los cambios pueden implicar tiempo de inactividad, se pueden utilizar estas ventanas para minimizar interrupciones de procesos comerciales importantes. En general, los cambios programados deben producirse dentro de una ventana de mantenimiento.

Ventana de desactivación

Indica un período de tiempo programado durante el cual no deberían producirse cambios en los elementos de configuración. Esta desactivación puede indicar un período de soporte reducido (por ejemplo, unas vacaciones), un evento corporativo o un momento importante del negocio como, por ejemplo, el cierre del ejercicio fiscal. En general, los cambios programados sólo deberían producirse fuera de las ventanas de desactivación.

3. (Opcional) Especifique los patrones de repetición de las ventanas para el cambio.
4. Abra el Calendario de cambios.
La leyenda muestra iconos y colores que identifican las ventanas para el cambio en la programación.
5. Cree órdenes de cambio asociadas a elementos de configuración.
6. Actualice el Calendario de cambios mediante el planificador de cambios.

Nota: Para obtener más información acerca de cómo crear ventanas para el cambio, consulte la *Ayuda en línea*.

Visualización de ventanas para el cambio

Puede ver ventanas para el cambio en el calendario de cambios para ver cuándo sus CI asociados pueden o no puede cambiarse.

Para ver ventanas para el cambio

1. En la ficha Administración, haga clic en Service Desk, Órdenes de cambio, Ventanas de cambio.
Aparecerá la lista de ventanas de cambio.
2. Seleccione la ventana para el cambio que desea ver.
Aparece la ventana para el cambio.
3. (Opcional) Haga clic en Editar.
Puede modificar la ventana para el cambio.
4. Guarde o cierre la ventana.
Aparece la página Detalles de ventana.

Cómo asociar un CI con una ventana de mantenimiento

Para controlar cuándo un CI se encuentra en mantenimiento, puede asociar ese CI a una ventana de mantenimiento.

Para asociar un CI con una ventana de mantenimiento

1. Vaya a la página Detalles de ventanas de cambio.
2. Haga clic en la ficha CI asociados.
Aparecerá la lista de CI asociados.
3. Haga clic en Actualizar elementos de configuración.
Aparecerá la página Búsqueda de CI.
4. Especifique información para los CI necesarios.
5. Haga clic en Buscar
Aparecerá la página CI disponibles.
6. Mueva algunos CI necesarios de la lista de CI disponibles a la lista de CI asociados.
7. Haga clic en OK.
Aparece la página Detalles de ventana para el cambio.
8. Haga clic en Guardar.
El CI se asocia con una ventana de mantenimiento.

Se guardan las asociaciones de ventanas seleccionadas, los CI y la ventana para el cambio.

Visualización de elementos de configuración asociados

Para determinar en qué CI se podría producir un impacto durante periodos específicos de tiempo, puede ver los CI que se asocian con ventanas de mantenimiento no globales.

Para ver CI asociados con una ventana de mantenimiento

1. Vaya a la página Detalles de ventanas de cambio.
2. Haga clic en la ficha CI asociados.
Se muestran los CI asociados.

Creación de un ejemplo de ventana de desactivación

El ejemplo siguiente demuestra cómo crear una ventana de desactivación para indicar que no deberían programarse órdenes de cambio durante un período de tiempo específico. Dicha ventana de desactivación durará 48 horas y se repetirá todos los viernes a las 6:00 de la tarde en su zona horaria.

Procedimiento para crear una ventana de desactivación

1. En la ficha Administración, haga clic en Service Desk, Órdenes de cambio, Ventanas de cambio.
Aparecerá la lista de ventanas de cambio.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nueva ventana de cambios.
3. Rellene los campos pertinentes como se indica a continuación:
 - a. Introduzca **Friday_Blackout** como nombre de la ventana.
 - b. Seleccione el tipo Desactivación.
 - c. Seleccione el estado Activo.
 - d. Seleccione el viernes próximo y las 6:00 de la tarde como Fecha de inicio en el Asistente de fecha.
 - e. Seleccione el domingo próximo y las 6:00 de la tarde como Fecha de finalización en el Asistente de fecha.
 - f. Seleccione su zona horaria.
 - g. (Opcional) Introduzca una descripción para la ventana de desactivación.
 - h. En la ficha Patrón de repetición, seleccione Semanal.
 - Establezca la repetición en cada **1** semana.
 - Seleccione la fecha en que terminará la repetición.
4. Guarde y cierre la ventana de desactivación.
5. Actualice la lista de ventanas de cambio.
6. Abra y actualice el calendario de cambios.
Aparecerá la ventana de desactivación en la programación.

Creación de una ventana de mantenimiento global

La página Lista de ventanas le permite ver y crear una ventana de mantenimiento global.

Para crear una ventana de mantenimiento global

1. Vaya a la página Lista de ventanas para el cambio.
2. Haga clic en Crear nuevo.
3. Aparecerá la página Crear nueva ventana de cambios.
4. Introduzca o modifique los campos necesarios para la ventana de mantenimiento.
5. Establezca el tipo en Mantenimiento
6. Verifique que la casilla de verificación Global esté marcada.

Nota: No puede asociarse una ventana de mantenimiento global con CI.

7. Introduzca la fecha de inicio, la fecha de finalización y la zona horaria.
8. Haga clic en Guardar.

Se guarda la ventana de mantenimiento global.

Detección de colisiones y análisis del conflicto

El análisis del conflicto detecta y muestra las colisiones que se producen cuando se programa la implementación de dos o más cambios en el mismo elemento de configuración al mismo tiempo. El equipo de gestión de cambios administra las colisiones de programación de las maneras siguientes:

- Utiliza el calendario de cambios para consultar las colisiones de CI relacionados con órdenes de cambio y hace ajustes en ellos para reducir la posible repercusión.
- Buscan y detectan las colisiones en un registro.

Nota: Para obtener más información acerca de cómo gestionar las colisiones de programación, consulte la *Ayuda en línea*.

Visualización de CA Workflow

La visualización del CA Workflow le permite controlar el progreso de tareas de workflow de orden de cambio. El visor de procesos muestra gráficamente cada paso del proceso de CA Workflow, lo cual incluye los pasos completos e incompletos y la ubicación actual de una progresión de workflow.

El visor de procesos muestra el estado y la ruta de acceso de procesos de CA Workflow cuando se asocia a una categoría de incidencias/cambios o a un área de problemas/incidentes/solicitudes.

Cómo visualizar el workflow

Visualice el workflow de la siguiente manera:

1. Asocie un proceso de CA Workflow a una categoría de cambios.
2. Cree una orden de cambio utilizando esa categoría de cambios.
3. En la ficha Tareas de workflow, haga clic en el botón Ver proceso para iniciar el visor de procesos.

Nota: Para obtener más información acerca de cómo asociar procesos de CA Workflow a categorías o áreas, consulte la *Ayuda en línea*.

Uso del ejemplo del visor de procesos

Este ejemplo demuestra cómo utilizar el visor de procesos en el sistema empleando una categoría de cambios predeterminada, después de instalar CA Workflow y de activar las opciones.

1. En la ficha Administración, desplácese a Service Desk, Órdenes de cambio, Categorías.
Aparecerá la página Lista de categorías de cambios.
2. Seleccione Add.IT.Other en la columna Símbolo.
Aparecerá la página Detalles de categoría de cambios Add.IT.Other.
3. Haga clic en Editar.
Aparecerá la página Actualizar categoría de cambios Add.IT.Other.
4. Haga clic en la ficha Workflow.
Haga clic en la casilla de verificación CA Workflow.
Aparecerá la lista de definiciones de workflow.
5. Seleccione Pedidos de equipos - Service Desk r12.5.
El nombre del proceso se incluye automáticamente en el campo Nombre de definición de CA Workflow.
6. Haga clic en Guardar.
Se actualizará la página Detalles de categoría de cambios.
7. Cierre la ventana.
8. Cree y guarde una orden de cambio utilizando la categoría Add.IT.Other.
La ficha Tareas de workflow muestra el proceso de Pedidos de equipos - Service Desk r12.5 y la Lista de elementos de trabajo.
9. Haga clic en el botón Ver proceso de la ficha Tareas de workflow.
Aparecerá el Visor de procesos.

Nota: Se puede ver el progreso actualizado de las tareas de workflow actualizando el Visor del procesos.

Definición de proceso de gestión de cambios para CA Workflow

La definición de proceso de gestión de cambios gestiona órdenes de cambio estándar, normales o de emergencia. Como parte de CA Workflow, la definición de proceso de gestión de cambios gestiona todas las tareas de orden de cambio desde la petición de cambio inicial, hasta la revisión posterior a la implementación. A medida que se completa cada tarea, la definición de proceso de gestión de cambios actualiza el estado de la orden de cambio y el registro de actividades. La definición de proceso de gestión de cambios también envía un correo electrónico al contacto o grupo sobre las tareas que requieren su finalización.

La definición de proceso de gestión de cambios incluye las siguientes funciones:

- Analiza el tipo de orden de cambio y el nivel de riesgo asociado para determinar el nivel necesario de aprobaciones para la implementación de cambios.
- Proporciona una base de muestra para la gestión de cambios.
- Se alinea con los estándares de ITIL v3 para la evaluación de riesgos, análisis de conflictos e impacto y aprobaciones tanto por el gestor de cambios como por el CAB.
- Incorpora la siguiente funcionalidad de gestión de cambios de CA Service Desk Manager:
 - Encuesta de evaluación de riesgo
 - Caso de negocio
 - Análisis del conflicto
 - Análisis del impacto
 - Códigos de cierre
 - Códigos de estado
 - Change Type
 - CAB e indicadores de aprobación de CAB

Más información:

[CA Workflow](#) (en la página 271)

Componentes de la definición de proceso de gestión de cambios

La definición de proceso de gestión de cambios tiene los siguientes componentes:

- **Definición de proceso de gestión de cambios:** definición de proceso que gestiona todo el proceso de órdenes de cambio. Todas las actividades y subactividades siguen las prácticas recomendadas de CA Workflow para el tratamiento de las excepciones. El nombre de archivo de la definición de proceso es *r12_Change_Mgmt_[en_language].xml*. Por ejemplo, el nombre de definición de proceso en inglés es *r12_Change_Mgmt_en_US.xml*.

Nota: Para obtener información sobre las prácticas recomendadas de CA Workflow, consulte

https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/7956/7956_tecdoc.html.

- **Definición de proceso de notificación y obtención de miembros de grupo:** elemento básico que gestiona las notificaciones de correo electrónico para los grupos. La definición de proceso de notificación y obtención de miembros acepta el UUID de grupo como entrada. Según el indicador de notificación, la definición de proceso de notificación y obtención de miembros de grupo puede enviar un correo electrónico a todos los miembros del grupo o solamente al gestor del grupo. El nombre de archivo de la definición de proceso es *r12_Get_Group_Mem_Notify_[en_language].xml*. Por ejemplo, el nombre de archivo de definición de proceso en inglés es *r12_Change_Mgmt_en_US.xml*.
- **Actor de notificación y obtención de miembros de grupo:** actor que invoca la definición de proceso de notificación y la obtención de miembros. El nombre de archivo del actor es *r12_Get_Group_Mem_Notify_Actor_[en_language].xml*. Por ejemplo, el nombre de archivo del actor en inglés es *r12_Get_Group_Mem_Notify_Actor_en_US.xml*.
- **Convertor de fecha y hora:** actor que acepta la fecha y hora como entrada y proporciona una cadena de fecha y hora legible para los campos de fecha de inicio de la planificación y la fecha de fin de la planificación en los formularios de aprobación. El actor del convertor de fecha y hora es un actor de JavaScript de CA Workflow. El nombre de archivo del actor es *r12_Date_Time_Convert_Actor_[en_language].xml*. Por ejemplo, el nombre de archivo del actor en inglés es *r12_Date_Time_Convert_Actor_en_US.xml*.

Cómo instalar la definición del proceso de gestión de cambios

Para instalar la definición del proceso de gestión de cambios, haga lo siguiente:

1. Use CA Workflow para revisar la documentación (see page 676) sobre los nodos de actividad, las subactividades y las notificaciones.
2. Cree el CAB y los grupos de implementación (see page 678) que son responsables de gestionar el proceso de cambio.
3. Cree contactos (see page 679) y asígneles al CAB o a los grupos de implementación.
4. Configure las notificaciones de correo electrónico (see page 677) para la definición del proceso de gestión de cambios.
5. Si no está utilizando el puerto de servidor Tomcat predeterminado 8090, configure el servidor Tomcat (see page 680) para las comunicaciones apropiadas entre CA Workflow y CA Service Desk Manager.
6. Configure una o más categorías de cambio (see page 681) para utilizar la definición de proceso de gestión de cambios.
7. Instale la opción Valores predeterminados de categoría (see page 682) en el gestor de opciones.

Consulte la documentación sobre nodos de actividad y atributos

Debido a que se documentan todos los atributos y nodos de actividad de la definición de proceso de gestión de cambios, se puede utilizar CA Workflow para ver información sobre los atributos y nodos de actividad. Si es necesario, se puede cambiar el flujo de la definición de proceso para cubrir las necesidades de la organización.

Nota: Para obtener información sobre la visualización de atributos y nodos de actividad, consulte la documentación de CA Workflow.

Procedimiento para visualizar la documentación sobre atributos y nodos de actividad

1. Abra la definición de proceso de la gestión de cambios de Service Desk r12.1 en la aplicación de CA Workflow.
Aparecerá la definición de proceso de gestión de cambios en CA Workflow.
2. Haga doble clic en un nodo de actividad.
Se abrirá el nodo de actividad.

3. En la ficha Propiedades, revise el campo Descripción para obtener detalles adicionales sobre el nodo.
4. Salga de las propiedades del nodo de actividad.
5. (Opcional) Vaya a la ficha Atributos en la ventana inferior de la definición de proceso.
6. Haga doble clic o mueva el ratón sobre el atributo.
Se abrirá la página Atributo con información sobre el atributo.

Visualización de subactividades

La definición de proceso de gestión de cambios utiliza varias subactividades de CA Workflow para simplificar el workflow. Si es necesario, mientras se trabaja con la definición de proceso de gestión de cambios, se pueden revisar y personalizar las subactividades.

Procedimiento para ver las subactividades

1. Abra la definición de proceso de la gestión de cambios de Service Desk r12.1 en la aplicación de CA Workflow.
Aparecerá la definición de proceso de gestión de cambios en CA Workflow.
2. Haga clic con el botón izquierdo en cualquier nodo con un signo más (+) y seleccione Abrir ficha o Abrir en línea.
Los detalles sobre la subactividad aparecen en una nueva ficha o junto a las actividades de definición de proceso.

Cómo configurar notificaciones por correo electrónico para los contactos de la gestión de cambios

El sistema envía notificaciones por correo electrónico sobre asignaciones de tareas de órdenes de cambio y cambios de estado. Las notificaciones por correo electrónico contienen vínculos a la lista de trabajo u orden de cambio para su revisión adicional. Dado que la definición del proceso de gestión de cambios envía notificaciones por correo electrónico, es necesaria la configuración del correo electrónico.

Si desea configurar las notificaciones por correo electrónico para los contactos de la gestión de cambios, realice lo siguiente:

1. En la ficha Administración, seleccione Gestor de opciones, Opciones de correo elec.
Aparecerá la lista de opciones.
2. Configure las opciones de correo electrónico según sea necesario para la organización.

Nota: Para obtener información sobre la configuración de correo electrónico, consulte la *Ayuda en línea*.

Cómo crear grupos de proceso de gestión de cambios

Cuando se creen grupos de proceso de gestión de cambios que sean responsables de aprobaciones y tareas adicionales, considere lo siguiente:

- Se puede utilizar cualquier nombre de grupo con la condición de que los nombres de CA Service Desk Manager y CA EEM coincidan.
- El nombre de grupo de CA Service Desk Manager también debe coincidir con el nombre de la carpeta de grupos en CA EEM.
- En cada grupo se requiere más de un miembro.
- Los miembros de grupo coinciden en CA Service Desk Manager y CA EEM. Por ejemplo, si el grupo de CAB de CA Service Desk Manager tiene cuatro miembros, el grupo de CAB de CA EEM tendrá los mismos miembros.

Nota: Para obtener información sobre la creación de grupos de CA Service Desk Manager y CA EEM, consulte la *Ayuda en línea* y la documentación de CA EEM.

Para crear grupos de gestión de cambios, realice lo siguiente:

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Grupos.
Aparecerá la página Búsqueda de grupos.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nuevo grupo.
3. Cree los siguientes grupos en CA Service Desk Manager:
 - **Grupo de CAB:** grupo de CAB que se asocia a la categoría de cambio o la orden de cambio.
 - **Grupo de implementación:** grupo de implementación que se asigna a la categoría de cambio o la orden de cambio.

4. Haga clic en Guardar.
Aparece la página Detalles del grupo.
5. Cree los mismos grupos en CA EEM.

Más información:

[Asignación de grupos de CAB](#) (en la página 696)

[Gestionar los grupos de CAB](#) (en la página 694)

Cómo crear contactos de proceso de gestión de cambios

Cuando se trabaja con la definición de proceso de gestión de cambios, se crean contactos que son responsables de las aprobaciones y tareas adicionales a lo largo del proceso de cambio. También se asignan los contactos a los grupos de procesos de gestión de cambios (see page 678).

Para crear los contactos de proceso de gestión de cambios, realice lo siguiente:

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Contactos.
Aparecerá la página Búsqueda de contactos.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nuevo contacto.
3. Cree los siguientes contactos con direcciones de correo electrónico válidas y asígnelos a los grupos apropiados:
 - **Solicitante:** uno o más contactos que envían la petición de cambio.
 - **Gestor de cambios:** el contacto que es el gestor del grupo de implementación. El grupo de implementación sólo puede tener un gestor de cambios.
 - **Gestor de CAB:** el contacto que es el gestor del grupo de CAB. El grupo de CAB sólo puede tener un gestor de CAB.La ficha Grupos de detalles de contacto muestra las asignaciones del grupo actual.
4. En la ficha Miembros de la página de detalles del grupo de implementación, configure el indicador Gestor para el gestor de cambios y el gestor de CAB.
5. Haga clic en Guardar.
La ficha Miembros muestra Gestor: Sí para los siguientes contactos:
 - Gestor de cambios
 - Gestor de CAB

6. Cree los mismos contactos en CA EEM y asígnelos a los grupos de CA EEM.

Nota: Los nombres de contacto pueden utilizar cualquier nombre de usuario o inicio de sesión de sistema que sea válido. Para obtener información sobre la creación de contactos de CA Service Desk Manager y CA EEM, consulte la *Ayuda en línea* y la documentación de CA EEM.

Especifique un puerto alternativo para el servidor Tomcat de CA Workflow

Si el servidor Tomcat de CA Workflow se está ejecutando en un puerto distinto al puerto predeterminado 8090, se debe configurar el puerto para que CA Workflow se comuniquen con CA Service Desk Manager.

Procedimiento para especificar un puerto alternativo para el servidor Tomcat de CA Workflow

1. Abra la aplicación de CA Workflow.
Aparece la página de CA Workflow.
2. Haga clic en la ficha Actores.
Aparece la lista Tipos de actores/Actores:
3. Seleccione JavaScript, USD_Initializer.
Aparece la página Opciones de actividad de CA Workflow.
4. Haga doble clic en la opción para obtener atributos globales.
Aparece la página de operación de JavaScript.
5. Cambie el valor de WFTomcatPort al puerto nuevo utilizado por CA Workflow Tomcat.
6. Haga clic en OK.
El servidor Tomcat se configura para que CA Workflow se comuniquen con CA Service Desk Manager.

Configuración de la categoría de cambio

Cuando se especifica la categoría de cambio para la definición de proceso de gestión de cambios, todas las nuevas órdenes de cambio que utilizan la categoría inician automáticamente la definición de proceso de gestión de cambios. Todos los valores de categoría de cambio configurados previamente, rellenan la orden de cambio de manera automática.

Procedimiento de configuración de la categoría de cambio

1. En la ficha Administración, seleccione Service Desk Manager, Órdenes de cambio, Categorías.
Aparecerá la lista de categorías de cambios.
2. Cree o abra una categoría de cambio existente.
Aparecerá la página Detalles de categoría de cambios.
3. En la ficha Workflow, haga clic Usar CA Workflow.
4. Haga clic en el vínculo Definición de CA Workflow.
Aparecerá la lista de definiciones de CA Workflow.
5. Haga el clic en la gestión de cambios de Service Desk r12.1.
6. Haga clic en OK.
Aparecerá la página Detalles de categoría de cambios.
7. (Opcional) Asigne CAB, Grupo y Encuesta de riesgos.
8. Haga clic en Guardar.
La nueva orden de cambio siguiente que utiliza esta categoría inicia automáticamente la definición de proceso de gestión de cambios con los valores de la categoría de cambio.

Nota: Para obtener información sobre cómo crear o editar categorías de cambio, consulte la *Ayuda en línea*.

Instale la opción Valores predeterminados de categoría en el gestor de opciones

La opción Valores predeterminados de categoría usa campos de categoría para completar CAB, Grupo y Encuesta de riesgo en la orden de cambio. Por ejemplo, el grupo CAB que especifica para una categoría aparece en todas las nuevas órdenes de cambio que utilizan la categoría.

Procedimiento para instalar la opción Valores predeterminados de categoría en el gestor de opciones

1. En la ficha Administración, seleccione Gestor de opciones, Gestor de órdenes de cambio, Valores predeterminados de categoría.
Aparecerá la Lista de opciones.
2. Haga clic con el botón secundario en Editar valores predeterminados de categoría.
Aparecerá la página Actualizar opciones de valores predeterminados de categoría.
3. Haga clic en Instalar.
4. Reinicie los servicios de CA Service Desk Manager.
Las nuevas órdenes de cambio automáticamente incluyen valores de la categoría.

Funcionamiento de la definición del proceso de gestión de cambios

Cuando un solicitante guarda una orden de cambio con una categoría que utiliza la definición del proceso de gestión de cambios, dicha definición se invoca de forma automática.

Los siguientes pasos describen el funcionamiento de la definición del proceso de gestión de cambios en CA Service Desk Manager:

1. El solicitante abre y guarda una orden de cambio que incluye la información siguiente:

Solicitante

Identifica la persona que abrió la orden de cambio.

Categoría de cambios

Identifica la categoría de orden de cambio.

Tipo

Identifica el tipo de orden de cambio como cambios estándares, normales o de emergencia. El tipo también se puede actualizar como parte del proceso de workflow.

Resumen/Descripción

Describe la razón de la orden de cambio.

Fecha de inicio planificada

Identifica la fecha de inicio.

Duración

Especifica el tiempo estimado para el cambio.

CI

Identifica por lo menos un CI afectado.

Se inicia la definición del proceso de gestión de cambios. El solicitante recibe una notificación por correo electrónico para rellenar la encuesta de evaluación de riesgos.

2. El solicitante revisa la orden de cambio y rellena la encuesta de evaluación de riesgos (see page 685) que describe la forma en que la orden de cambio afecta a los servidores, aplicaciones y usuarios.

La definición del proceso de gestión de cambios analiza las respuestas para determinar el riesgo y garantizar que la orden de cambio siga la ruta de proceso apropiada. El solicitante recibe una notificación por correo electrónico para realizar el análisis de impactos y conflictos.

3. Durante el análisis de impactos y conflictos (see page 686), el solicitante busca conflictos de planificación y analiza el impacto de la orden de cambio en los CI.

El solicitante recibe una notificación por correo electrónico para realizar el análisis de cambios.

4. Durante el análisis de cambios (see page 687), el solicitante identifica y envía el tipo de cambio, el motivo del cambio, el impacto en el negocio y el impacto general del cambio.

El gestor de cambios recibe una notificación por correo electrónico para aprobar la orden de cambio. Si la orden de cambio es un riesgo alto, el grupo de CAB también recibe una notificación.

5. El gestor de cambios revisa el análisis de cambios e introduce comentarios sobre la revisión. El gestor de cambios aprueba, rechaza o marca la orden de cambio como incompleta (see page 686).

El sistema actualiza la página Detalles de orden de cambio según sea necesario y responde con una de las siguientes acciones:

- Si la orden de cambio está aprobada y no se necesita ninguna aprobación de CAB, el grupo de implementación recibe una notificación. La orden de cambio muestra el estado Aprobado.
 - Si la orden de cambio está aprobada y se necesitan más aprobaciones de CAB, los miembros y el gestor de CAB reciben una notificación para la aprobación. La orden de cambio muestra el estado Aprobación en curso.
 - Si la orden de cambio está rechazada, muestra el estado Rechazado.
 - Si la orden de cambio está marcada como incompleta, muestra el estado Incompleto.
6. En el caso de las órdenes de cambio aprobadas, un miembro del grupo de implementación confirma el inicio de la implementación (see page 690) e implementa el cambio.

La orden de cambio muestra el estado Implementación en curso.

7. Una vez finalizado el trabajo, el gestor de implementación completa la revisión posterior a la implementación (see page 691) para describir los detalles sobre el resultado del cambio.

CA Workflow cierra la orden de cambio. La orden de cambio muestra un código de cierre y el estado Implementado.

Más información:

[Cómo instalar la definición del proceso de gestión de cambios](#) (en la página 676)

[Cómo implementar la encuesta sobre riesgos](#) (en la página 699)

[Visualización de encuestas sobre riesgos predeterminadas](#) (en la página 700)

Cómo gestiona aprobaciones de CO la definición del proceso de CM

El siguiente diagrama muestra cómo la definición del proceso de gestión de cambios (see page 682) gestiona las aprobaciones para una nueva orden de cambio.

Cómo gestiona implementaciones de CO la definición del proceso de CM

El siguiente diagrama muestra cómo la definición del proceso de gestión de cambios (see page 682) gestiona las implementaciones de órdenes de cambio.

Rellenado de la encuesta de evaluación de riesgos

Al crear una orden de cambio, el sistema le indica que rellene la encuesta de evaluación de riesgos asociada con la categoría de cambio. Como solicitante, puede identificar, evaluar y cuantificar los riesgos de las órdenes de cambio que pertenecen a categorías de cambio antes de modificar un sistema o servicio.

Procedimiento para rellenar la encuesta de evaluación de riesgos

1. Abra la orden de cambio. Para ello, haga clic en el vínculo de notificación por correo electrónico de la encuesta de evaluación de riesgos.
Aparecerá la página Detalles de orden de cambio.
2. En la ficha Tareas de workflow, haga clic en el vínculo de la encuesta de evaluación de riesgos del solicitante y siga las instrucciones para rellenar la encuesta.
Aparecerá la lista de trabajo de CA Workflow.
3. En la ficha Tareas, haga clic en el vínculo Ejecutar.
Aparecerá la página de ejecución de tareas.
4. Tome nota de las instrucciones y haga clic en el vínculo.
Aparecerá la Encuesta sobre riesgos.
5. Responda detenidamente las preguntas de la encuesta para que el workflow de procesos de gestión de cambios pueda evaluar con precisión la ruta de riesgo adecuada para el cambio.
6. Haga clic en Enviar.
Aparecerá la página de ejecución de tareas.
7. Haga clic en Confirmar.
La página Detalles de orden de cambio muestra el estado Petición de cambio. El solicitante recibe una notificación por correo electrónico para realizar el análisis de impactos y conflictos.

Más información:

[Cómo acceder a una encuesta de riesgos directamente desde una URL](#) (en la página 701)

Realización de análisis de impactos y conflictos

Durante el análisis de impactos y conflictos, el solicitante busca conflictos de planificación y analiza el impacto de la orden de cambio en los CI.

Procedimiento para realizar el análisis de impactos y conflictos

1. Abra la orden de cambio. Para ello, haga clic en el vínculo de notificación por correo electrónico.
Aparecerá la página Detalles de orden de cambio.
2. En la ficha Tareas, haga clic en el vínculo de análisis de impactos y conflictos del solicitante.
Aparecerá la página de tareas.
3. En la ficha Tareas, haga clic en el vínculo Ejecutar.
Aparecerá la página de ejecución de tareas.
4. Tome nota de las instrucciones del análisis de impactos y conflictos, y haga clic en el vínculo.
Aparecerá la página Detalles de orden de cambio.
5. En la ficha de conflictos de orden de cambio, haga clic en Análisis del conflicto para resolver todos los conflictos destacados y de planificación. Resuelva todos los conflictos antes de implementar el cambio.
Aparece la Lista de conflictos.
6. En la ficha Elementos de configuración, haga clic en Análisis de impactos para revisar los detalles acerca de los CI.
Aparece la lista de elementos de configuración.
7. En la ficha Elementos de configuración, haga clic en Explorador de impactos para revisar la información acerca de cada CI.
Se abre el Explorador de impactos.
8. Haga clic en Visualizador para obtener una vista gráfica de las relaciones de CI.
Nota: El botón Visualizador sólo está disponible cuando CA CMDB está instalado.
9. Vuelva a la página de ejecución de tareas y haga clic en Confirmar.
La ficha Tareas de workflow muestra un vínculo para iniciar el análisis de cambios. El solicitante recibe una notificación por correo electrónico para realizar el análisis de cambios.

Más información:

[Explorador de impactos](#) (en la página 702)

[Inicio del Visualizador de CMDB desde Explorador de impactos](#) (en la página 706)

Realización del análisis de cambios

Durante el análisis de cambios, el solicitante identifica y registra la siguiente información:

- Tipo de cambio
- Motivo del cambio
- Impacto del negocio
- Impacto general del cambio

Procedimiento para realizar el análisis de cambios

1. Abra la orden de cambio. Para ello, haga clic en el vínculo de notificación por correo electrónico.

Aparecerá la página Detalles de orden de cambio.

2. En la ficha Tareas de workflow, haga clic en el vínculo del formulario de análisis de cambios del solicitante.

Aparecerá la página de tareas.

3. En la ficha Tareas, haga clic en el vínculo Ejecutar.

Aparece la página de análisis de cambios.

4. En la ficha de análisis de cambios, responda las preguntas para confirmar la orden de cambio y haga clic en Enviar. Por ejemplo, resuma el análisis y explique el objetivo de la orden de cambio. En caso de ser necesario, especifique si la orden de cambio es una repetición o un reproceso. Resuma el impacto del negocio y el impacto general del cambio.

En función del riesgo y del tipo de cambio, el sistema realiza las siguientes acciones:

- Si el tipo de cambio es normal con un riesgo de alto a extremo, la página Detalles de orden de cambio muestra lo siguiente:
 - Aprobación de CAB: Sí
 - Estado: Aprobación en curso

El sistema indica al gestor de cambios que apruebe la orden de cambio. Una vez que se tenga la aprobación del gestor de cambios, se notifica al grupo de CAB para una aprobación adicional.

- Si el tipo de cambio es normal con un riesgo de medio a bajo, la página Detalles de orden de cambio muestra lo siguiente:
 - Aprobación de CAB: No
 - Estado: Aprobación en curso

El sistema indica al gestor de cambios que apruebe la orden de cambio.

- Si el tipo de cambio es estándar, el sistema indica al grupo de implementación que implemente el cambio.
- Si el tipo de cambio es de emergencia, la página Detalles de orden de cambio muestra Aprobación de CAB: No.

El sistema notifica a ECAB. Una vez que ECAB haya procesado la orden de cambio, la página Detalles de orden de cambio muestra el estado Aprobación en curso y el gestor de cambios recibe una notificación para aprobar la orden de cambio.

Cómo aprobar, rechazar o marcar órdenes de cambio como incompletas

El tipo de la orden de cambio y el nivel de riesgo dirigen el proceso de aprobación de órdenes de cambio que utilizan la definición del proceso de gestión de cambios. Los siguientes valores de orden de cambio determinan los aprobadores de órdenes de cambio:

- Si el tipo es normal y el riesgo es de medio a bajo, la orden de cambio sólo necesita la aprobación del gestor de cambios.
- Si el tipo es normal y el riesgo es de alto a extremo, la orden de cambio requiere la aprobación de un miembro del CAB.
- Si el tipo es estándar, no se requiere aprobación. El sistema notifica al grupo Implementación para que trabaje en la orden de cambio.
- Si el tipo es emergencia, el sistema notifica al grupo de ECAB. La orden de cambio muestra el estado en Aprobación en curso. Cuando la orden de cambio está preparada para aprobación, el sistema notifica al gestor de cambios.

Como aprobador, revise la información de análisis de cambio y decida aprobar, rechazar o marcar la orden de cambio como incompleta.

Procedimiento para aprobar, rechazar o marcar una orden de cambio como incompleta

1. Abra la orden de cambio; para ello, haga clic en el vínculo de notificación del correo electrónico.

Aparecerá la página Detalles de orden de cambio.

2. En la ficha Tareas de workflow, haga clic en el vínculo del formulario de aprobación del gestor de cambios.
Aparecerá la página Tareas.
3. En la ficha Tareas, haga clic en el vínculo para ejecutar.
Aparece la página de CAB o de Aprobación del gestor de cambios.
4. Revise la ficha de análisis de cambios para obtener información adicional sobre la orden de cambio.
5. Según el nivel de aprobación necesario, seleccione una de las fichas de aprobación siguientes y responda las preguntas de aprobación:

Aprobación del gestor de cambios

Describe la decisión del gestor de cambios para la orden de cambio.

Aprobación de CAB

Describe la decisión del aprobador de CAB para la orden de cambio.

6. Seleccione uno de los siguientes niveles de aprobación:

Aprobar

Acepta la orden de cambio.

Rechazar

Rechaza la orden de cambio.

Incompleto

Marca la orden de cambio como incompleta.

Aparece la página Resultado. Según el nivel de aprobación, ocurren las acciones siguientes:

- Si aprueba la orden de cambio y no se requiere ninguna otra aprobación de CAB, la página Detalles de orden de cambio muestra el estado Aprobado y el grupo Implementación recibe una notificación para empezar a trabajar.
- Si aprueba la orden de cambio y se requiere la aprobación de CAB, la página Detalles de orden de cambio muestra el estado Aprobación en curso. El grupo de CAB también recibe una notificación.
- Si rechaza la orden de cambio, la página Detalles de orden de cambio muestra el estado Rechazado y el solicitante y el grupo de implementación reciben una notificación.
- Si la orden de cambio está incompleta, la página Detalles de orden de cambio muestra el estado Incompleto y el solicitante recibe una notificación.

Más información:

[Funcionamiento de procesos de CAB](#) (en la página 642)

[Responsabilidades de CAB](#) (en la página 642)

[Aprobaciones de CAB](#) (en la página 696)

Implementación de una orden de cambio

Para una orden de cambio en particular, un grupo de implementación completa uno o más elementos de trabajo. Como miembro del grupo de implementación, notifica la información sobre el cambio.

Procedimiento para implementar una orden de cambio

1. Inicie sesión en CA Service Desk Manager como miembro del grupo de implementación y abra la orden de cambio.
Aparecerá la página Detalles de orden de cambio.
2. En la ficha Tareas de workflow, haga clic en el vínculo para implementar la orden de cambio.
Aparecerá la página Lista de tareas.
3. En la ficha Tareas, haga clic en el vínculo para ejecutar.
Aparecerá la página para ejecutar tareas.
4. Siga las instrucciones para revisar la orden de cambio y haga clic en Confirmar.
La página Detalles de orden de cambio muestra el estado Implementación en curso.
5. Implementar el cambio. Por ejemplo, si la orden de cambio solicitaba instalar el parche del antivirus en el servidor de Exchange 1 y el servidor de Exchange 2, complete la orden de cambio de acuerdo con las directrices y los estándares de la compañía.
6. En la ficha Tareas de workflow, haga clic en el vínculo para implementar el formulario completo.
Aparecerá la página Tareas.
7. En la ficha Tareas, haga clic en el vínculo para ejecutar.
Aparece la página Implementación completa.
8. En la ficha de implementación completa, responda las preguntas para describir cómo su grupo implementaba la orden de cambio y haga clic en una de las opciones siguientes:

Finalizada

Especifica todas las tareas de orden de cambio completadas con éxito. Establece el estado de la orden de cambio en Implementación completa y el código de cierre en Correcto.

Incompleto

Especifica que uno o más elementos de la orden de cambio no pudieron completarse.

El solicitante recibe una o más notificaciones sobre si se completó o revirtió la orden de cambio. El sistema también responde en una de las siguientes formas:

- Si se completó la orden de cambio, la página Detalles de orden de cambio muestra lo siguiente:

- Estado: implementación completa
- Código de cierre: correcto

El sistema notifica al grupo de implementación para que complete la revisión posterior a la implementación.

- Si no se completó la orden de cambio, la página Detalles de orden de cambio muestra lo siguiente:

- Estado: revertido
- Código de cierre: incorrecto

El sistema también notifica al grupo de implementación para que determine si la acción de revertir fue correcta.

Cuando la acción de revertir fue correcta, el sistema notifica al grupo de implementación para que complete la revisión posterior a la implementación. Si la acción de revertir no es correcta, el sistema crea un incidente y notifica al grupo de implementación para que complete la revisión posterior a la implementación.

Cómo completar la revisión posterior a la implementación

Una vez finalizado el trabajo, el grupo de implementación completa la revisión posterior a la implementación que describe los detalles sobre el resultado del cambio. Como miembro del grupo de implementación, normalmente puede completar la revisión posterior a la implementación de tres a siete días posteriores a la implementación de la orden de cambio. Sin embargo, la definición del proceso de gestión de cambios establece un retraso predeterminado de diez segundos para la asignación de esta tarea.

Procedimiento para completar la revisión posterior a la implementación

1. Inicie sesión en CA Service Desk Manager como miembro del grupo de implementación y abra la orden de cambio.
Aparecerá la página Detalles de orden de cambio.
2. En la ficha Tareas de workflow, haga clic en el vínculo de la revisión posterior a la implementación.
Aparecerá la Lista de tareas.
3. En la ficha Tareas, haga clic en el vínculo Ejecutar.
Aparecerá la página de la revisión posterior a la implementación.
4. En la ficha de la revisión posterior a la implementación, responda las preguntas para describir la resolución y haga clic en Enviar.
La página Detalles de orden de cambio muestra el estado Cerrado.

No se encontró el actor ActivityNode: actualice el objeto -Service Desk r12

Síntoma:

La ventana de comando de CA Workflow muestra el siguiente error:

No se encontró el actor ActivityNode: actualice el objeto -Service Desk r12

Solución:

1. Inicie sesión en la aplicación CA Workflow.
2. Haga clic en la ficha Actores.
3. Seleccione la carpeta de procesos.
4. Seleccione Archivo/Nuevo actor.
5. Seleccione Actualizar objeto -Service Desk r12 en la lista desplegable.
6. Haga clic en OK.

Como parte de la definición del proceso de gestión de cambios, el sistema utiliza al nuevo actor.

No se cierra la orden de cambio

Síntoma:

Durante el último paso en el workflow, la orden de cambio no se cierra. La instancia de proceso de CA Workflow muestra el estado En ejecución y CA Workflow informa un error de falla de Actor.

Solución:

Al cerrar la orden de cambio, verifique que haya configurado todos los campos obligatorios, por ejemplo la causa raíz.

Generación de informes y Consola de CAB

La Consola de CAB es un panel que facilita la rápida aprobación en línea de órdenes de cambio que requieren la aprobación de CAB. El Gestor de cambios y otros miembros de CAB utilizan la consola para ver detalles de órdenes de cambio (y de sus tareas de workflow y elementos de configuración asociados) y aprobarlas o rechazarlas. La Consola de CAB permite a los miembros del equipo revisar, aprobar o rechazar una orden de cambio y pasar rápidamente a la siguiente orden de cambio. En el caso de solicitudes de órdenes de cambio, el CAB puede tratar la solicitud satisfaciéndola directamente o escalándola/remitiéndola a un grupo pertinente.

El Gestor de cambios puede utilizar opciones de generación de informes pormenorizados y de resumen integradas en CA Service Desk Manager para hacer lo siguiente:

- Informar de órdenes de cambio aprobadas y rechazadas.
- Informar de órdenes de cambio a la espera de aprobación.

Para imprimir o ver los informes de resumen y detallados, seleccione primero los registros que se deseen incluir en el informe en cuestión. Para hacerlo, se puede usar la función de búsqueda de las páginas de lista.

Así, por ejemplo, es posible indicar criterios de búsqueda en la Lista de órdenes de cambio para crear una lista de órdenes de cambio a la espera de aprobación por el CAB aptas para la generación del informe.

Nota: Para obtener más información sobre cómo generar informes detallados y de resumen en CA Service Desk Manager, consulte la información de Generación de informes de la *Ayuda en línea*.

Más información:

[Gestionar los grupos de CAB](#) (en la página 694)

[Asignación de grupos de CAB](#) (en la página 696)

[Aprobaciones de CAB](#) (en la página 696)

[Modificación de las propiedades de la Consola de CAB](#) (en la página 696)

[Informe de gestión de cambios](#) (en la página 698)

Gestionar los grupos de CAB

Se pueden crear y gestionar grupos de CAB con los miembros pertinentes en relación con las órdenes de cambio que se estén considerando. El CAB puede incluir a miembros del equipo de aplicaciones, el gestor de desarrollo, el propietario del componente, control de calidad, soporte y cualquier otra parte que se estime necesaria.

Nota: Antes de implementar un grupo de CAB, configure los contactos apropiados para su estructura empresarial.

Procedimiento para crear grupos de CAB

1. En la ficha Administración, seleccione Grupos.
Aparecerá la página Búsqueda de grupos.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nuevo grupo.
3. Rellene los campos según sea necesario.
4. Haga clic en Guardar.
El Grupo de CAB aparece en la página Lista de grupos.

Procedimiento para asignar miembros al grupo de CAB

1. En la página Detalles de grupo, seleccione la ficha Miembros.
2. Haga clic en Actualizar miembros.
Aparecerá la página Búsqueda de contactos.
3. Introduzca los criterios de búsqueda para mostrar los contactos deseados y haga clic en Buscar.
Aparecerá la página Actualización de miembros, que muestra los contactos que coinciden con los criterios de búsqueda.
4. Seleccione en la lista de la izquierda los contactos que desee asignar a este grupo. Para seleccionar varios elementos, mantenga pulsada la tecla Ctrl mientras hace clic con el botón izquierdo del ratón.

5. Cuando haya seleccionado todos los contactos que desee, haga clic en el botón de selección ($\geq$).

Los contactos seleccionados se mueven a la lista de miembros a la derecha.

6. Haga clic en OK.

Aparecerá la página Detalles de grupo, que muestra los contactos seleccionados en la ficha Miembros.

Procedimiento para agregar el grupo de CAB a una categoría de cambios

Nota: Asegúrese de que esté instalada la opción Category_Defaults, para que el campo CAB sobre órdenes de cambio adquiera de forma predeterminada el valor de un grupo de CAB.

1. En la ficha Administración, seleccione CA Service Desk Manager, Órdenes de cambio, Categorías.

Aparecerá la lista de categorías de cambios.

2. Seleccione una categoría de la lista.

Aparecerá la página Actualizar categoría de cambios.

3. Seleccione el grupo de CAB apropiado del campo CAB.

4. Rellene el resto de campos según sea necesario.

5. Haga clic en Guardar.

La página Detalles de categoría de cambios mostrará un mensaje que indicará que se ha guardado correctamente.

6. Haga clic en Cerrar ventana.

Se asocia el grupo de CAB a la categoría de cambios y la orden de cambio.

Más información:

[Orden de cambio y categorías de incidencia](#) (en la página 295)

[Area Defaults](#) (en la página 430)

Asignación de grupos de CAB

Se puede asignar un grupo de CAB para revisar una orden de cambio antes de implementarla.

Procedimiento para asignar grupos de CAB a órdenes de cambio

1. Seleccione la orden de cambio deseada de la lista de órdenes de cambio.
Aparecerá la página Detalles de orden de cambio.
2. Haga clic en Editar.
3. Seleccione CAB en el área de detalles.
Aparecerá la página Lista de grupos.
4. Seleccione un grupo de CAB.
5. Haga clic en Guardar, Cerrar ventana.
Se asigna el grupo de CAB a la orden de cambio.

Aprobaciones de CAB

El comité Change Advisory Board (CAB) debe aprobar una orden de cambio antes de implementarla si se establece el campo Aprobación de CAB como SÍ. Durante el proceso de aprobación, cuando el gestor de cambios hace clic en Aprobar o Rechazar, el estado de la orden de cambio se modifica a Aprobado o Rechazado, respectivamente.

Nota: Si quiere utilizar diferentes valores de estado, puede actualizar el código del botón Aprobar o Rechazar utilizando Web Screen Painter.

Más información:

[Modificación de las propiedades de la Consola de CAB](#) (en la página 696)

Modificación de las propiedades de la Consola de CAB

Utilizando Web Screen Painter, se pueden cambiar las propiedades de la Consola de CAB que aparecen en los formularios Web de ésta. Por ejemplo, se puede hacer lo siguiente:

- Cambiar el nombre de los botones Aprobar y Rechazar. Estos botones son propiedades de los formularios Web `orderwf_approval_console.htmlpl` (tareas de CA Workflow) y `order_approval_console.htmlpl` (órdenes de cambio).

- Personalice los valores de estado de los botones Aprobar y Rechazar cambiando los valores "REJ" o "APR".
 - El botón "Rechazar tarea" llama a una función `approve_reject('REJ')`.
 - El botón "Aprobar tarea" llama a una función `approve_reject('APR')`.

Importante: Puede asociar solamente una transición activa con un botón. No desactive una transición de estado predefinida que esté asociada con un botón, o de lo contrario, la transición de estado predefinida ya no funcionará.

Procedimiento para modificar las propiedades de la Consola de CAB

1. En Web Screen Painter, abra el formulario de la Consola de CAB que desee cambiar.

Web Screen Painter abre y muestra el formulario.

2. En la ficha Diseño, haga clic con el botón derecho en el control que desee cambiar y seleccione Propiedades.

Aparecerá la página de *control* Propiedades.

3. Cambie las propiedades que desee introduciendo un valor nuevo para cada una.

Los cambios entran en vigor al hacer clic fuera del campo y cuando se cierra la página Propiedades.

Web Screen Painter muestra un breve resumen del significado de las propiedades mediante una nota que aparece en la parte inferior del formulario Propiedades al seleccionar una propiedad concreta.

Nota: Para obtener información sobre Web Screen Painter, consulte la *Guía de implementación*.

Ejemplo: Personalización de la Consola de CAB para tareas de workflow de cambios

Este ejemplo muestra cómo personalizar el estado de tareas utilizando Web Screen Painter.

1. En Web Screen Painter, abra el formulario Web `orderwf_approval_console.html`.

Web Screen Painter abre y muestra el formulario.

2. En la ficha Diseño, haga clic con el botón derecho en el botón Rechazar tarea y seleccione Propiedades.

Aparecerá la página Propiedades: Botón.

3. Busque la función `approve_reject('REJ')`.

'REJ' es el código de estado de tarea Rechazar.

4. Introduzca un valor nuevo para 'REJ'.

Los cambios entran en vigor al hacer clic fuera del campo y cuando se cierra la página Propiedades.

Web Screen Painter muestra un breve resumen del significado de las propiedades mediante una nota que aparece en la parte inferior del formulario Propiedades al seleccionar una propiedad concreta.

Informe de gestión de cambios

El gestor de cambios, con los privilegios pertinentes, puede utilizar BusinessObjects InfoView para acometer lo siguiente:

- Informar del volumen de cambios por sistema operativo, categoría de cambios, grupo, implementador, riesgo, estado, fecha de implementación, elementos de configuración afectados y cambios que se originan a partir de tickets de problemas o incidentes.
- Informar los cambios implementados con éxito agrupados por la categoría de cambio, la urgencia, la prioridad, el impacto, el porcentaje de éxito comparado con el total para el periodo especificado y el grupo de solicitantes de cambio.
- Informar cambios que presentaron fallos agrupados por la categoría, la urgencia, la prioridad, el impacto, la razón para la cancelación, el porcentaje de fallo comparado con el total para el periodo especificado y el grupo de solicitantes de cambio.
- Informar del número total de solicitudes de cambios agrupado por coordinador de cambios de la categoría de cambios, gestor de cambios, nivel de riesgo, prioridad y elementos de configuración afectados de un período de tiempo específico.

Puede desplazarse a los informes predefinidos del panel izquierdo de la ventana InfoView para ver, programar, modificar o ejecutar los informes o para ver el historial y las propiedades de estos.

Nota: Para obtener más información acerca del uso de BusinessObjects InfoView, consulte la información de CA Business Intelligence en la *Ayuda en línea*.

Evaluación de riesgos

Las evaluaciones de riesgos permiten identificar, evaluar y cuantificar los riesgos de órdenes de cambio que pertenecen a categorías de cambios, antes de modificar un sistema o servicio de su entorno. Se crean encuestas para evaluar los riesgos y asociarlas a categorías de cambios. Cuando un usuario crea una orden de cambio y especifica una categoría de cambios, la encuesta asociada a dicha categoría estará disponible para su cumplimentación y envío.

La encuesta sobre riesgos incluye una serie de preguntas tipo test o para responder libremente. Cada respuesta tiene un valor de ponderación. Al crear una orden de cambio, el usuario selecciona las respuestas apropiadas y envía la encuesta. El nivel de riesgo evaluado se basa en las ponderaciones de las respuestas seleccionadas por el usuario.

Más información:

[Visualización de encuestas sobre riesgos predeterminadas](#) (en la página 700)

[Implementación de un ejemplo de encuesta sobre riesgos](#) (en la página 700)

Cómo implementar la encuesta sobre riesgos

Implemente la encuesta sobre riesgos de la siguiente manera:

1. Establezca los niveles del riesgo de su organización.
2. Cree o seleccione una encuesta sobre riesgos de la lista predeterminada.
3. Cree o modifique las preguntas y respuestas de la encuesta sobre riesgos.
4. Modifique los intervalos de riesgo de la encuesta sobre riesgos.
5. Asocie la encuesta sobre riesgos a una categoría de cambios.
6. Después de asociar una encuesta sobre riesgos a una categoría de cambios, aparecerá el botón Encuesta sobre riesgos para el solicitante cuando éste guarde una orden de cambio utilizando la categoría de cambios especificada.
7. Vea el riesgo evaluado según los resultados de la encuesta sobre riesgos.
8. (Opcional) Omita el valor del riesgo evaluado del menú Actividades.

Nota: Para obtener más información acerca de cómo crear y modificar encuestas sobre riesgos, consulte la *Ayuda en línea*.

Visualización de encuestas sobre riesgos predeterminadas

CA Service Desk Manager ofrece encuestas sobre riesgos predeterminadas que pueden asociarse a categorías de cambios.

Procedimiento para ver las encuestas sobre riesgos predeterminadas

1. Desplácese a Service Desk, Órdenes de cambio, Encuesta sobre riesgos.
2. Seleccione General en la columna Nombre de la encuesta sobre riesgos.
Aparecerá la página Detalles de encuesta de riesgo general.
3. Haga clic en Ver encuesta.
Aparecerá la encuesta sobre riesgos, con preguntas, respuestas y valores de ponderación de cada respuesta. Esta encuesta se aplica a los cambios generales dentro de su organización.
4. Cierre la encuesta.
5. Aparecerá la página Detalles de encuesta de riesgo general; ciérrela.

Implementación de un ejemplo de encuesta sobre riesgos

Este ejemplo demuestra cómo implementar una encuesta sobre riesgos predeterminada en el sistema utilizando una categoría de cambios predeterminada.

1. Desplácese a Service Desk, Órdenes de cambio, Categorías.
Aparecerá la lista de categorías de cambios.
2. Seleccione Add.IT.Other en la columna Símbolo.
Aparecerá la página Detalles de categoría Add.IT.Other.
3. Haga clic en Editar.
Aparecerá la página Actualizar categoría de cambios Add.IT.Other.
4. Haga clic en Encuesta sobre riesgos
Aparecerá Búsqueda de plantilla de encuesta de riesgo.
5. Busque la encuesta sobre riesgos. En este ejemplo, busque General y seleccione la encuesta sobre riesgos para agregarla al formulario de detalles.
El campo Encuesta sobre riesgos se rellena con General.
6. Guarde y cierre la ventana.

Si un usuario crea una orden de cambio utilizando la categoría Add.IT.Other, cuando la guarde aparecerá el botón Encuesta sobre riesgos.

Cómo acceder a una encuesta de riesgos directamente desde una URL

Puede proporcionar una URL dinámica para permitir que un usuario acceda a una encuesta de riesgos de orden de cambio directamente a través de una URL desde una tarea en CA Workflow. Puede añadir esta URL dinámica con el parámetro *KEEP.UsingURL=1* para indicar que se está accediendo a la encuesta de riesgos directamente con una URL.

Cree la URL dinámica en CA Workflow de la siguiente forma:

1. Abra la definición de proceso de CA Workflow y agregue el nodo de actividad para que un usuario complete la encuesta de riesgos.
2. En el nodo de actividad, agregue una URL dinámica con la sintaxis apropiada. Verifique que se añade el parámetro *KEEP.UsingURL=*, como en el siguiente ejemplo:

```
http://<nombrehost>:<puerto>/CAisd/pdmweb.exe?CNT_ID=<ID de
contacto>+CRID=<ID de orden de cambio>+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
```

nombre de host

Especifica el nombre de host del servidor de CA Service Desk Manager.

puerto

Especifica el puerto en el que se instala CA Service Desk Manager.

ID de contacto

Especifica el ID interno del contacto que completa la encuesta de riesgos.

ID de la orden de cambio

Especifica el ID interno de la orden de cambio asociada con la encuesta de riesgos.

En el siguiente ejemplo aparece una URL de muestra:

```
http://nombrehost:8080/CAisd/pdmweb.exe?CNT_ID=21A7CC606A3011DEA39AA8010000A8
00+CRID=400009+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
```

Importante: si no agrega el parámetro *KEEP.UsingURL=1* a la URL dinámica, el usuario recibirá un mensaje de error tras enviar la encuesta de riesgos y no se calculará el nivel de riesgo.

3. Guarde la definición de proceso de CA Workflow.
4. Cree una categoría de cambio y asocie una encuesta de riesgos y la definición de proceso de CA Workflow a la categoría de cambio.
Guarde los cambios.
5. Abra una orden de cambio con esta categoría de cambio y guárdela para crear una instancia del proceso de CA Workflow.

6. Como parte del proceso de CA Workflow, se asigna un usuario a una tarea para completar la encuesta de riesgos. El usuario hace clic en la URL, como se señaló anteriormente.
7. El usuario se conecta a CA Service Desk Manager mediante la URL y aparece directamente en el contexto de la encuesta de riesgo para la orden de cambio.
8. El usuario envía la encuesta y aparece un mensaje que indica si el envío fue correcto o erróneo.

Si es correcto, el nivel de riesgo se calcula y se actualiza en la orden de cambio.

Explorador de impactos

Explorador de impactos es una herramienta avanzada para gestionar y controlar cambios dentro de una organización. Explorador de impactos permite al gestor de cambios explorar los elementos de configuración adjuntos a una orden de cambio y también interactuar directamente con un elemento de configuración adjunto o con sus elementos de configuración secundarios.

Explorador de impactos ofrece estas ventajas:

- muestra todos los elementos de configuración adjuntos a una orden de cambio;
- muestra todas las relaciones de punto a punto y secundarias de los elementos de configuración adjuntos;
- ofrece la capacidad de adjuntar a la orden de cambio cualquier elemento de configuración relacionado;
- muestra una lista de descendientes de los elementos de configuración relacionados sucesivamente para cualquier elemento de configuración adjunto;
- ofrece la capacidad de iniciar el Visualizador de CMDB para un CI.

Más información:

[Inicio de Explorador de impactos](#) (en la página 703)

[Exploración de los elementos de configuración adjuntos](#) (en la página 703)

[Visualización de elementos de configuración en Explorador de impactos](#) (en la página 704)

[Cómo agregar un elemento de configuración relacionado a una orden de cambio](#) (en la página 705)

[Cómo mostrar la lista de descendientes de elementos de configuración](#) (en la página 705)

[Inicio del Visualizador de CMDB desde Explorador de impactos](#) (en la página 706)

[Configuración de Explorador de impactos](#) (en la página 706)

Inicio de Explorador de impactos

Se puede acceder a Explorador de impactos desde la ficha Elementos de configuración de cualquier orden de cambio.

Procedimiento para iniciar Explorador de impactos

1. Abra la página Detalles de orden de cambio.
2. Seleccione la configuración. Elementos de configuración.
3. Haga clic en Explorador de impactos.

Aparecerá la página Explorador de impactos.

Nota: Si cierra la página Detalles de orden de cambio, también se cierra la página de Explorador de impactos.

Nota: Si se inicia Explorador de impactos desde varias órdenes de cambio, aparecerán varias páginas de Explorador de impactos.

Exploración de los elementos de configuración adjuntos

El árbol de Explorador de impactos contiene un nodo para cada elemento de configuración adjunto a una orden de cambio. El signo más (+) indica que un elemento de configuración tiene por lo menos un elemento de configuración secundario.

Nota: Si se adjuntan más de 100 elementos de configuración a la orden de cambio, sólo aparecerán los 100 primeros.

Para mostrar las relaciones de un elemento de configuración adjunto, haga clic en el signo más (+) del elemento de configuración. Los elementos de configuración relacionados aparecen en el árbol. Además de los nombres de elementos de configuración relacionados, el árbol también muestra tipos de relación entre paréntesis.

Nota: Si la orden de cambio tiene más de 100 elementos de configuración adjuntos, sólo se mostrarán los 100 primeros. Para ver los 100 elementos de configuración siguientes, haga clic en Más...

Visualización de elementos de configuración en Explorador de impactos

El árbol de Explorador de impactos muestra un nodo para cada elemento de configuración vinculado a una orden de cambio. El signo más (+) indica que un elemento de configuración tiene por lo menos un elemento de configuración secundario.

Procedimiento para ver elementos de configuración

1. Haga clic en un nodo de elemento de configuración del panel izquierdo.

Aparecerá la página Detalles de elemento de configuración en el panel derecho.

Nota: También puede ver la página Detalles de CI en el panel derecho haciendo clic con el botón derecho del ratón en el CI y seleccionando Ver en el menú contextual.

2. Haga clic en el nodo de orden de cambio de la parte superior del panel izquierdo.

Aparecerá la página Detalles de orden de cambio.

Nota: Si la orden de cambio tiene más de 100 elementos de configuración adjuntos, sólo se mostrarán los 100 primeros. Para ver los 100 elementos de configuración siguientes, haga clic en Más...

Cómo agregar un elemento de configuración relacionado a una orden de cambio

Al explorar las relaciones de los elementos de configuración, tal vez desee adjuntar un elemento de configuración relacionado a la orden de cambio.

Procedimiento para agregar un elemento de configuración relacionado a una orden de cambio

1. Haga clic en la ficha Elementos de configuración de una orden de cambio.
Aparecerá la página Lista de elementos de configuración.
2. Haga clic en Explorador de impactos.
El árbol de Explorador de impactos muestra elementos de configuración adjuntos.
3. Haga clic en cualquier más (+) de un nodo de elementos de configuración adjuntos
Aparecen los elementos de configuración relacionados con el nodo.
4. Haga clic con el botón derecho en un elemento de configuración relacionado y seleccione Agregar a orden de cambio en el menú contextual.
Aparecerá el nuevo elemento de configuración adjunto en la página Elementos de configuración de la orden de cambio.

Cómo mostrar la lista de descendientes de elementos de configuración

Se pueden mostrar las líneas de elementos de configuración relacionados (denominados *descendientes*) en relación con cualquier elemento de configuración. Además de la información básica sobre cada elemento de configuración, la lista de descendientes de elementos de configuración muestra los niveles de relación, con el elemento de configuración de origen como nivel 1. Los elementos secundarios de elementos de configuración empiezan en el nivel 2, sus elementos secundarios en el 3, y así sucesivamente. Si se encuentra un elemento de configuración más de una vez entre las relaciones trazadas, sólo se muestra su nivel de relación más próximo.

Ejemplo: Varias rutas de descendientes relativas a un elemento de configuración

Debido a las diversas relaciones, una búsqueda de descendientes encuentra el mismo elemento de configuración relacionado en el nivel 2 y también en el nivel 4. El elemento de configuración descendiente sólo aparece en el nivel 2.

Procedimiento para listar descendientes de un elemento de configuración

1. Desde una página Detalles de orden de cambio, seleccione la ficha Elementos de configuración.
2. Haga clic en Explorador de impactos para ver los elementos de configuración adjuntos.
3. Si es necesario, expanda un nodo de elemento de configuración.
4. Haga clic con el botón derecho en un elemento de configuración y seleccione Listar descendientes.

Aparecerá la lista de descendientes de elementos de configuración.

Inicio del Visualizador de CMDB desde Explorador de impactos

El explorador de impactos ofrece la capacidad de iniciar el Visualizador de CMDB de un CI adjunto o relacionado.

Para iniciar el Visualizador de CMDB desde el explorador de impactos

1. Desde una página Detalles de orden de cambio, haga clic en Explorador de impactos.

Aparecerá la página Explorador de impactos.

2. Haga clic con el botón derecho en cualquier elemento de configuración y seleccione Inicio del visualizador en el menú contextual.

Se inicia el Visualizador de CMDB con el CI como foco.

Configuración de Explorador de impactos

Un Administrador puede configurar Explorador de impactos de la siguiente manera:

- Especifique el número de elementos de configuración secundarios que aparecen en relación con un elemento de configuración adjunto.
- Especifique el número de niveles de relación que aparecen en la lista de descendientes de elemento de configuración.
- Suprima la visualización de elementos de configuración secundarios.

Se puede configurar el número de elementos de configuración secundarios mostrado agregando un parámetro `NX_IMPACT_EXPLORER_MAX_CHILD_NODES` al archivo de configuración `NX.env`. El valor predeterminado es 100.

Ejemplo: Configuración de la visualización de elementos de configuración secundarios

Si se emplea la configuración siguiente, Explorador de impactos sólo muestra diez elementos secundarios a la vez para un elemento de configuración adjunto:

```
@NX_IMPACT_EXPLORER_MAX_CHILD_NODES=10
```

La profundidad predeterminada de la lista de descendientes de elementos de configuración es de nueve (9) niveles. Se puede configurar la profundidad agregando un parámetro `NX_IMPACT_EXPLORER_MAX_LEVELS` al archivo de configuración `NX.env`.

Ejemplo: Configuración del número de niveles de descendientes

Si se utiliza la configuración siguiente, la lista de descendientes de elementos de configuración muestra el elemento de configuración de origen y sólo los elementos de configuración anexos mediante relaciones:

```
@NX_IMPACT_EXPLORER_MAX_LEVELS=2
```

Utilice la opción siguiente del gestor de opciones para suprimir la visualización de un cierto tipo de elemento de configuración secundario:

```
IMPACT_EXPLORER_EXCLUDE_HIER=boolean
```

Si la opción `IMPACT_EXPLORER_EXCLUDE_HIER` está instalada y definida como **Sí**, los CI secundarios relacionados a través de la ficha Relaciones CMDB de una página Detalles de CI no aparecen en el árbol del explorador de impactos ni en lista de descendientes de los elementos de configuración (CI).

Nota: Todavía se muestran los CI secundarios que se relacionan por medio de CA CMDB.

Capítulo 17: Gestión de informes de CA Business Intelligence

Esta sección contiene los siguientes temas:

[Informes de CA Business Intelligence](#) (en la página 709)
[Escenarios de generación de informes](#) (en la página 710)
[Componentes de los informes](#) (en la página 711)
[Diagrama de flujo de datos de informes](#) (en la página 713)
[Visualización de informes en InfoView](#) (en la página 714)
[Seguridad y autorización](#) (en la página 714)
[Cómo dirigir un servidor existente de CA Business Intelligence a un servidor de CA Service Desk Manager](#) (en la página 719)
[Cómo configurar la seguridad de partición de datos para la generación de informes](#) (en la página 722)
[Base de datos replicada para la generación de informes sin conexión](#) (en la página 724)
[Informes de Role-Based](#) (en la página 725)
[Informes basados en Web](#) (en la página 734)
[Informes de cuadros de mandos](#) (en la página 738)
[Informes ad hoc](#) (en la página 739)
[Indicadores clave de rendimiento](#) (en la página 747)
[Escritura de informes de CA Business Intelligence](#) (en la página 759)

Informes de CA Business Intelligence

CA Business Intelligence es un componente basado en Web que incorpora la tecnología de objetos de negocio, integrada con CA Service Desk Manager y una variedad de orígenes de datos comunes, como por ejemplo SQL Server, Oracle y Open Database Connectivity (ODBC).

CA Business Intelligence utiliza BusinessObjects Enterprise XI como el sistema de informes predeterminado. Los informes predefinidos se proporcionan para CA Service Desk Manager, Gestión del conocimiento y Automatización de soporte.

Gracias a los informes de CA Business Intelligence, los usuarios pueden hacer lo siguiente:

- Personalizar informes existentes
- Obtener detalles sobre datos de informes de objetos de negocio para mostrar los datos debajo de diagramas y grupos resumidos

- Exportar instancias de informes a diferentes formatos de salida
- Generar informes ad hoc
- Publicar nuevos informes y distribuirlos a usuarios autorizados
- Programar informes para que se ejecuten en los horarios especificados
- Utilizar la generación de informes del cuadro de mandos para controlar las operaciones diarias de todos los tipos de ticket de CA Service Desk Manager.

Nota: El acceso a la generación de informes está restringido a través de la seguridad de partición de datos de CA Service Desk Manager.

Escenarios de generación de informes

CA Business Intelligence integrado con BusinessObjects Enterprise admite los siguientes escenarios de generación de informes:

- **Informes basados en roles:** en la ficha Informes de CA Service Desk Manager, los usuarios autorizados pueden ver los informes definidos para su rol y gestionar sus informes personales en BusinessObjects InfoView haciendo clic en el botón InfoView. CA Service Desk Manager utiliza la interfaz de InfoView para recopilar, organizar y presentar la información en formatos de informe. En InfoView, los informes predefinidos se agrupan en carpetas públicas.
- **Informes basados en Web:** los informes basados en Web son informes predefinidos de CA Service Desk Manager, Gestión del conocimiento, CMDB y Automatización de soporte. Éstos se desarrollan mediante Web Intelligence o Crystal Reports. Se accede a los informes en InfoView y se pueden utilizar como modelos para definir los informes específicos del sitio.
- **Informes ad hoc:** los informes ad hoc se crean y administran en InfoView mediante una interfaz basada en complementos de Web Intelligence. Puede almacenar y gestionar los informes en un espacio de trabajo personal (Mis Carpetas). Los informes ad hoc están destinados a los usuarios que desean crear informes básicos de forma sencilla sin escribir consultas.
- **Informes de cuadro de mandos:** los informes de cuadro de mandos permiten controlar operaciones diarias para todos los tipos de ticket de CA Service Desk Manager (solicitud/incidente/problema, orden de cambio o incidencia) en InfoView. Cada informe contiene un análisis sobre los principales realizadores que trabajan en tickets activos, de modo que sea posible controlar su progreso. Puede trabajar por separado con informes de cuadros de mandos predefinidos o utilizar el cuadro de mandos corporativo para ver todas las operaciones diarias de CA Service Desk Manager en una sola vista.

Componentes de los informes

BusinessObjects Enterprise y sus herramientas asociadas, junto con Crystal Reports XI de BusinessObjects, son la red troncal de la arquitectura de CA BI.

Aunque se proporcionan informes de Crystal Reports como el componente principal de CA Business Intelligence, la herramienta de creación y mantenimiento de informes, Crystal Reports XI, no se proporciona como parte de CA Business Intelligence. Crystal Reports XI es un producto con licencia independiente que se puede comprar en BusinessObjects Enterprise y que se utiliza junto con CA Business Intelligence.

Nota: CA Service Desk Manager ya no desarrolla ni proporciona informes predefinidos de Microsoft Access.

Puede utilizar los siguientes componentes para administrar, controlar y configurar el entorno de generación de informes de CA Business Intelligence:

- **Base de datos de CA Service Desk Manager/Domsrvr/Controlador ODBC:** los datos de los informes se almacenan en una base de datos de CA Service Desk Manager Oracle o SQL Server. Las aplicaciones de informes BusinessObjects (Crystal Reports y Web Intelligence) acceden a la base de datos mediante un controlador ODBC que se conecta directamente con el motor de objetos de CA Service Desk Manager (domsrvr). Toda la seguridad de CA Service Desk Manager, incluidas la partición de datos y las restricciones de clientes, se aplica automáticamente a los informes, pero no al entorno de generación de informes. Puede configurar el entorno de generación de informes de forma que funcione con las particiones de datos existentes en CA Service Desk Manager.

Nota: Si desea obtener información sobre cómo establecer seguridad de particiones de datos para el entorno de generación de informes, consulte *Cómo configurar la seguridad de partición de datos para la generación de informes* (see page 714).

- **Servidor de gestión central (CMS):** repositorio central que almacena todos los objetos utilizados en cada proceso de la generación de informes.
- **Consola de gestión central:** componente administrativo que proporciona acceso a todas las funciones de administración de BusinessObjects. Si utiliza CMC, puede desplegar informes y asignar permisos de carpeta y acceso para InfoView. Las opciones de autenticación, roles y permisos de usuario deben establecerse en el entorno de generación de informes mediante CMC.

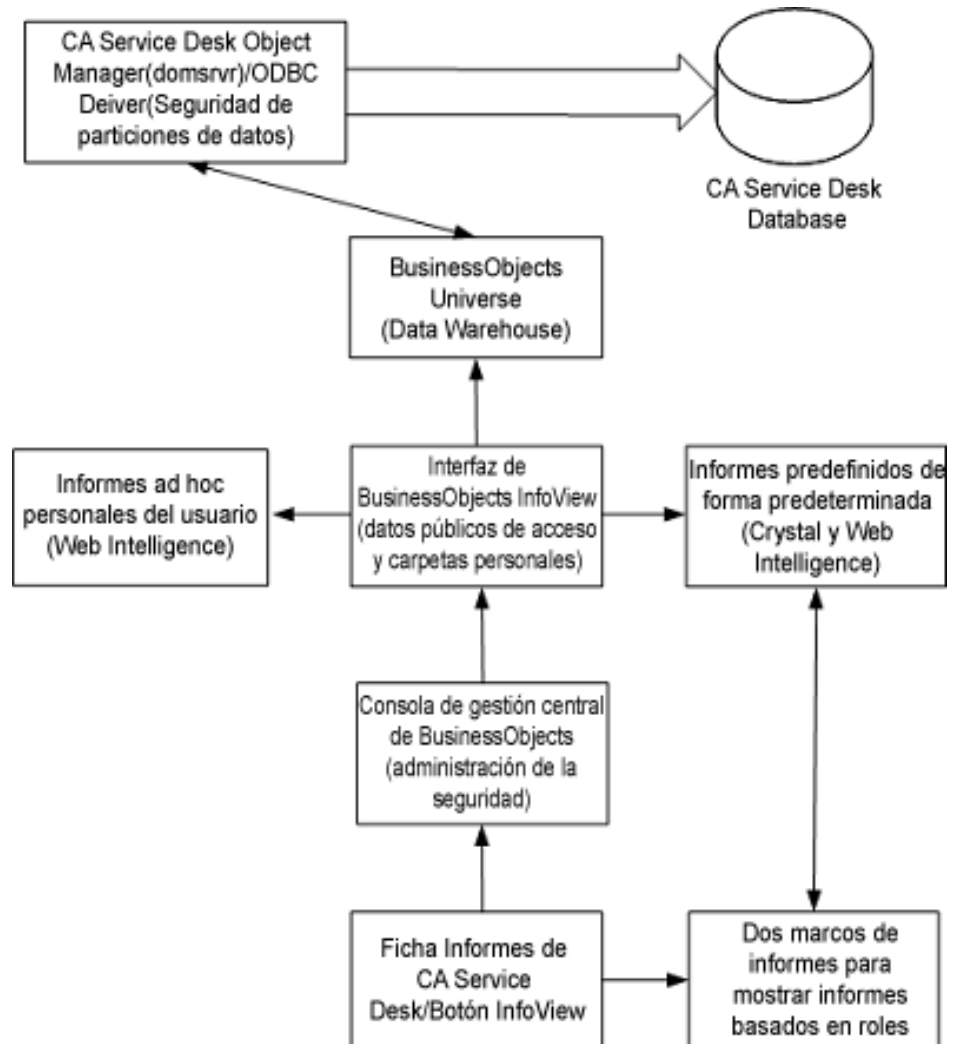
Nota: Las opciones de autenticación, roles y permisos de usuario deben establecerse en el entorno de generación de informes antes de utilizar CA Business Intelligence. Para obtener más información sobre cómo definir la seguridad, consulte *Seguridad y autenticación* (see page 714).

- **Universo de BusinessObjects:** describe las clases (tablas) y los objetos (columnas) que se utilizan en los informes. El universo de CA Service Desk Manager se instala y se configura durante la instalación. Al completarse la instalación, la conexión de universos se asigna a diversos grupos y usuarios en CA Service Desk Manager.
 - **Designer:** componente de BusinessObjects que permite modificar el universo de CA Service Desk Manager. Se trata de una metacapa entre el esquema de CA Service Desk Manager y las herramientas de generación de informes de BusinessObjects. El Asistente de importación/exportación facilita la extracción o relleno de objetos dentro del CMS.
 - **Informes predefinidos predeterminados:** los informes predefinidos son informes basados en Web de CA Service Desk Manager y de Gestión del conocimiento creados con Web Intelligence o Crystal Reports. Los informes se pueden utilizar como modelos para definir los informes específicos del sitio.
 - **InfoView:** BusinessObjects InfoView es una interfaz Web que permite a los usuarios autorizados de CA Service Desk Manager interactuar con informes Web predefinidos viendo, ejecutando y programando tipos de informes, como, por ejemplo, informes de Web Intelligence y de Crystal Reports, entre otros. Los informes se incluyen en carpetas en la sección pública de InfoView.
 - **Informes ad hoc:** los informes ad hoc permiten crear y administrar informes mediante una interfaz basada en complementos de Web Intelligence. Esta herramienta está destinada a los usuarios que desean crear informes básicos de forma sencilla sin escribir consultas.
- Nota:** Para ver ejemplos de uso de informes ad hoc, consulte Informes ad hoc (see page 739).
- **Informes de cuadro de mandos:** los informes de cuadro de mandos permiten controlar operaciones diarias para todos los tipos de ticket de CA Service Desk Manager (solicitud/incidente/problema, orden de cambio o incidencia) en BusinessObjects InfoView. Cada informe contiene un análisis sobre los principales realizadores que trabajan en tickets activos, de modo que sea posible controlar su progreso.
 - **Ficha Informes de CA Service Desk Manager:** los usuarios autorizados pueden ver en esta ficha los informes basados en roles y, a continuación, hacer clic en el botón InfoView de la ficha para gestionar sus informes personales en InfoView.

Nota: Para obtener información sobre cómo gestionar informes basados en roles y mostrar nuevos informes en la ficha Informes, consulte Informes basados en Web (see page 734).

Diagrama de flujo de datos de informes

El siguiente diagrama ilustra la ejecución y el flujo de datos de los componentes para CA Business Intelligence integrado en BusinessObjects Enterprise:



Visualización de informes en InfoView

Los informes predefinidos de CA Service Desk Manager que aparecen en BusinessObjects InfoView se encuentran en las carpetas públicas. Puede expandir las carpetas para ver cualquier subcarpeta. Cada informe contiene vínculos que permiten a los usuarios ver, ver el historial, programar y modificar los informes, como se muestra en el siguiente ejemplo.

Asset					
Organizar ▾		Filtro: Todos los tipos ▾			
	Título ▲	Última ejecución	Tipo	Propietario	Instancias
☐	Asset List	Nunca ejecutado	Crystal Reports	Administrator	0
	Historial Programar Propiedades Modificar This report shows the Resource Family (Hardware, Software etc), the type of Asset (keyboard, modem,etc), the serial number for that Asset, a more detailed description of the Asset.				

Nota: Para obtener información sobre el uso de informes en InfoView, consulte la *Guía del usuario de BusinessObjects InfoView*.

Seguridad y autorización

La configuración de seguridad predeterminada para BusinessObjects Enterprise se realiza mediante la configuración de CA Business Intelligence. La configuración determina las políticas de seguridad de carpetas, universos, conexiones de universos y herramientas. También proporciona métodos para agregar usuarios y asignarlos a grupos, así como para establecer algunas opciones de preferencias.

Específicamente, la configuración de informes de CA Business Intelligence implica:

- Configuración de seguridad
- Implementación de informes
- Implementación de universos
- Configuración de las opciones de inteligencia Web

Al completarse la instalación, la conexión de universos se asigna a diversos grupos y usuarios en CA Service Desk Manager.

El administrador puede iniciar sesión en la CMC de BusinessObjects y modificar la configuración predeterminada en cualquier momento. Los usuarios están autorizados para acceder a las carpetas de InfoView en función del grupo de CA Business Intelligence al que pertenecen.

Grupos y usuarios

Durante la configuración de CA Business Intelligence, se agregarán al servidor de gestión central (CMS) los grupos enumerados en la tabla que se muestra a continuación. Se relacionan con los roles de CA Service Desk Manager con los mismos nombres. Durante la fase de configuración de CA Business Intelligence, una casilla de verificación opcional estaba disponible para indicar si los usuarios de muestra se agregan a CMS. Si se activó, la configuración predeterminada de CMS incluye un usuario de muestra por cada grupo. En CMC, puede utilizar estos usuarios de muestra como modelos al establecer permisos de usuario y opciones de autenticación para el entorno de generación de informes.

Nombre de grupo	Nombre de usuario
Gestor de cambios	Usuario gestor de cambios
Gestor de servicio al cliente	Usuario gestor del servicio al cliente
Gestor de conocimientos	Usuario gestor de conocimientos
Analista de conocimiento	Usuario analista de conocimiento
Service Desk Manager	Usuario de Service Desk Manager
Gestor de incidentes	Usuario gestor de incidentes
Gestor de problemas	Usuario gestor de problemas

Nota: Estos usuarios de muestra existirán solamente si se solicitan durante la configuración de CA Business Intelligence.

Universo y conexiones de universos

La configuración predeterminada también incluye la política de seguridad para acceder al universo de CA Service Desk Manager y las conexiones de universos. Para permitir acceso completo, todos los grupos predeterminados se definen para tener acceso de control total.

Nombre de grupo	Nivel de acceso
Gestor de cambios	Control total
Gestor de servicio al cliente	Control total
Analista de conocimiento	Control total
Gestor de conocimientos	Control total
Service Desk Manager	Control total

Nombre de grupo	Nivel de acceso
Gestor de incidentes	Control total
Gestor de problemas	Control total

Carpetas de informes

La configuración predeterminada viene con un conjunto de carpetas que contienen informes predefinidos para CA Service Desk Manager y Gestión del conocimiento. Cada grupo de CA Service Desk Manager se configura para tener acceso a un subconjunto de estas carpetas.

Nombre de carpeta	Nombre de grupo	Nivel de acceso
Agregar	■ Gestor de cambios	■ Vista
	■ Gestor de servicio al cliente	■ Vista
	■ Gestor de conocimientos	■ Ningún acceso
	■ Analista de conocimiento	■ Ningún acceso
	■ Service Desk Manager	■ Control total
	■ Gestor de incidentes	■ Vista
	■ Gestor de problemas	■ Vista
Activo	■ Gestor de cambios	■ Vista a petición
	■ Gestor de servicio al cliente	■ Vista
	■ Gestor de conocimientos	■ Ningún acceso
	■ Analista de conocimiento	■ Ningún acceso
	■ Service Desk Manager	■ Control total
	■ Gestor de incidentes	■ Vista
	■ Gestor de problemas	■ Vista
Orden de cambio (incluye todas las subcarpetas)	■ Gestor de cambios	■ Control total
	■ Gestor de servicio al cliente	■ Ningún acceso
	■ Gestor de conocimientos	■ Ningún acceso
	■ Analista de conocimiento	■ Ningún acceso
	■ Service Desk Manager	■ Vista
	■ Gestor de incidentes	■ Vista
	■ Gestor de problemas	■ Vista

Nombre de carpeta	Nombre de grupo	Nivel de acceso
Incidencia (incluye todas las subcarpetas)	■ Gestor de cambios	■ Ningún acceso
	■ Gestor de servicio al cliente	■ Control total
	■ Gestor de conocimientos	■ Ningún acceso
	■ Analista de conocimiento	■ Ningún acceso
	■ Service Desk Manager	■ Ningún acceso
	■ Gestor de incidentes	■ Ningún acceso
	■ Gestor de problemas	■ Ningún acceso
Solicitud (incluye todas las subcarpetas)	■ Gestor de cambios	■ Ningún acceso
	■ Gestor de servicio al cliente	■ Ningún acceso
	■ Gestor de conocimientos	■ Ningún acceso
	■ Analista de conocimiento	■ Ningún acceso
	■ Service Desk Manager	■ Control total
	■ Gestor de incidentes	■ Vista
	■ Gestor de problemas	■ Ningún acceso
Gestión del conocimiento	■ Gestor de cambios	■ Ningún acceso
	■ Gestor de servicio al cliente	■ Vista
	■ Gestor de conocimientos	■ Control total
	■ Analista de conocimiento	■ Vista
	■ Service Desk Manager	■ Programación
	■ Gestor de incidentes	■ Vista
	■ Gestor de problemas	■ Vista
Estudio	■ Gestor de cambios	■ Ningún acceso
	■ Gestor de servicio al cliente	■ Ningún acceso
	■ Gestor de conocimientos	■ Vista
	■ Analista de conocimiento	■ Ningún acceso
	■ Service Desk Manager	■ Control total
	■ Gestor de incidentes	■ Vista
	■ Gestor de problemas	■ Vista
Gestión de problemas e incidentes	■ Gestor de cambios	■ Ningún acceso
	■ Gestor de servicio al cliente	■ Ningún acceso
	■ Gestor de conocimientos	■ Vista

Nombre de carpeta	Nombre de grupo	Nivel de acceso
	■ Analista de conocimiento	■ Ningún acceso
	■ Service Desk Manager	■ Programación
	■ Gestor de incidentes	■ Control total
	■ Gestor de problemas	■ Control total

Niveles de acceso

La configuración predeterminada incluye los siguientes niveles de acceso para grupos y usuarios:

Ningún acceso

Establece todos los permisos en Sin especificar.

Vista

Permite que el usuario vea la carpeta, informe o universo. Si el informe contiene datos, el usuario puede abrirlo e interactuar con él. Si el informe no contiene datos, el usuario no puede actualizarlo. De forma predeterminada, el usuario puede editar el informe, guardarlo en una carpeta personal y actualizarlo ahí. Puede impedir explícitamente que otros usuarios copien documentos corporativos a carpetas personales si establece un derecho individual que deniegue "Copiar objetos a otra carpeta".

Programación

Permite al usuario programar informes pero no actualizarlos en tiempo real.

Vista a petición

Permite al usuario actualizar informes en tiempo real. Cuando el informe es un documento de Web Intelligence, el usuario también necesita acceso de Vista a petición al universo y la conexión de universos para llevar a cabo la actualización.

Control total

Permite al usuario crear nuevos informes dentro de una carpeta, modificar informes existentes o suprimir elementos.

Avanzada

Cuando los niveles de acceso anteriores no cubren sus necesidades, proporcionamos acceso más granular al elegir Avanzado.

Cuando un nivel de acceso de grupo o usuario se establece en Avanzado, se pone a disposición más control granular de derechos que los que se asignan mediante la selección de Vista, Programación, Vista a petición o Control total.

Las carpetas de BusinessObjects utilizan seguridad heredada. El usuario recibe la misma autoridad en las carpetas de nivel inferior y en las carpetas de nivel superior asignadas a él o a su grupo, a menos que las restricciones de sustitución se apliquen en niveles inferiores. Se proporcionan autorizaciones predeterminadas en el nivel de carpeta y nivel de grupo. Los usuarios heredarán los derechos de su grupo para todos los objetos en la carpeta y las carpetas subordinadas.

CA Business Intelligence se instala con dos grupos: Administrators y Everyone. Al grupo Everyone se le asigna un nivel de acceso de Programación que permite programar y ver todos los objetos de informes.

Más información:

[Carpetas de informes](#) (en la página 716)

Cómo dirigir un servidor existente de CA Business Intelligence a un servidor de CA Service Desk Manager

Si tiene un servidor existente de CA Business Intelligence, lo puede dirigir a un servidor de CA Service Desk Manager como se indica a continuación:

1. Cree una fuente de datos ODBC. (see page 719)
2. Configure el universo (see page 721).
3. Exporte el universo. (see page 721)
4. Inicie InfoView para verificar la conexión.

Creación de una fuente de datos ODBC

Para crear un origen de datos ODBC utilice el Administrador de orígenes de datos ODBC.

Procedimiento para crear nuevos orígenes de datos ODBC

1. Desplácese a Inicio, Todos los programas, Herramientas administrativas, Orígenes de datos (ODBC).

Se abre el Administrador de orígenes de datos ODBC:

2. Seleccione la ficha DSN de sistema y haga clic en Agregar.

Aparecerá la página para crear un nuevo origen de datos.

3. Seleccione DataDirect OpenAccess y haga clic en Finalizar.

Aparece la página de instalación de DataDirect OpenAccess ODBC.

4. Especifique *casd_servername* en el campo Nombre de ODBC.

5. Haga clic en Avanzadas.

Aparece la página Avanzadas.

6. Haga clic en Agregar.

Aparece la página de instalación de la base de datos de OpenAccess.

7. Rellene los siguientes campos:

- **Nombre.** Especifique *casd_servername*.

- **Dirección IP.** Especifique *servername* o la dirección IP.

Nota: Haga ping en *servername* para determinar su dirección IP a fin de utilizar la dirección IP en lugar de *servername*.

- **Puerto.** Especifique 1706.

- **Tipo.** (Opcional) Especifique la base de datos empleada en el servidor. Este campo se utiliza solamente como información de referencia.

8. Haga clic en OK.

9. Seleccione *casd_servername* en la lista desplegable de la base de datos.

10. Haga clic en OK.

Se crea el origen de datos ODBC.

Configuración del universo.

Después de crear el origen de datos ODBC, necesita configurar el universo estableciendo una conexión entre CA Service Desk Manager y CA Business Intelligence.

Procedimiento para configurar el universo

1. Inicie Designer e inicie sesión como administrador.
2. Haga clic en Archivo, Importar.
Aparecerá la página de Importar universo.
3. Examine y seleccione el universo de CA Service Desk Manager y haga clic en Aceptar.
Aparecerá un mensaje que indica que se importó correctamente el universo.
4. Haga clic en Archivo, Parámetros.
Aparecerá la página de parámetros de universo.
5. Haga clic en Editar.
Aparecerá la página Editar conexión de CA Service Desk Manager.
6. Especifique el nombre del usuario y la contraseña del usuario con privilegios de CA Service Desk Manager, como ServiceDesk.
7. Seleccione `casd_servername` en el nombre del origen de datos y haga clic en Siguiente.
8. Haga clic en Probar conexión para verificar que el universo de CA Service Desk Manager se comunica con CA Business Intelligence.
9. Haga clic en Siguiente, Siguiente, Finalizar.
El universo queda configurado.

Exportación del universo

Después de configurar el universo, necesita exportarlo desde Designer.

Procedimiento para exportar el universo

1. Haga clic en Archivo, Exportar.
Aparecerá el cuadro de diálogo Exportar universo.
2. Haga clic en Continuar.
3. Haga clic en OK.
Se exporta el universo.

Cómo configurar la seguridad de partición de datos para la generación de informes

El acceso a la generación de informes de CA Business Intelligence se restringe mediante la *Seguridad de partición de datos* de CA Service Desk Manager. Toda la seguridad de CA Service Desk Manager, incluidas la partición de datos y las restricciones de cliente, se aplica automáticamente a los informes.

La seguridad de partición de datos para el entorno específico de generación de informes no se aplica durante la fase de configuración. Puede configurar el entorno de generación de informes de forma que funcione con las particiones de datos existentes en CA Service Desk Manager.

Para dicha tarea, utilice las siguientes herramientas:

- **Consola de gestión central de BusinessObjects (CMC):** permite administrar permisos y autenticación de usuario de BusinessObjects Enterprise.
- **BusinessObjects Designer:** permite modificar el universo de CA Service Desk Manager, Gestión del conocimiento, CMDB y Automatización de soporte. Se trata de una metacapa entre el esquema de CA Service Desk Manager y las herramientas de generación de informes.
- **Gestión de seguridad y de roles de CA Service Desk Manager:** permite configurar la seguridad de partición de datos para determinar los datos a los que pueden acceder los usuarios.

Más información:

[Adición de un usuario con privilegios de CA Service Desk Manager a CMC](#) (en la página 723)

[Definición de las credenciales de la base de datos de universo](#) (en la página 723)

[Establecimiento de particiones de datos](#) (en la página 724)

Adición de un usuario con privilegios de CA Service Desk Manager a CMC

La conexión de universos se configura de forma predeterminada para utilizar la contraseña y el usuario con privilegios de Service Desk al acceder datos. Este usuario se debería agregar a CMC como nuevo usuario de CA Business Intelligence. Este usuario se agrega con dos objetivos. Primero, necesita a este usuario si piensa configurar la seguridad de partición de datos para la generación de informes; en segundo lugar, podrá utilizar a este usuario cuando pruebe los informes en la ficha Informes de CA Service Desk Manager. La ficha Informes requiere un usuario definido tanto en CA Service Desk Manager como en CA Business Intelligence.

Utilice las instrucciones proporcionadas en la *Guía de implementación* para agregar a los usuarios de CA Service Desk Manager a CMC y para configurar la cuenta de usuario con privilegios de CA Service Desk Manager.

Definición de las credenciales de la base de datos de universo

El universo debe utilizar las credenciales de base de datos asociadas con la cuenta de usuario de BusinessObjects.

Nota: Verifique que inicia sesión en BusinessObjects Designer con la cuenta del usuario con privilegios y no con la cuenta del usuario administrador.

Procedimiento para definir las credenciales de la base de datos de universo

1. En el menú Inicio, vaya a BusinessObjects XI Release2, BusinessObjects Enterprise, Designer.
Aparecerá la ventana Diseñador.
2. Inicie sesión en Designer.
Aparecerá la ventana Diseñador.
3. Seleccione Archivo, Importar.
Aparecerá el cuadro de diálogo Importar universo.

4. Seleccione la carpeta de universos de CA Service Desk Manager, Gestión del conocimiento, CMDB o Automatización de soporte en la lista desplegable.

Nota: Si ésta es la primera vez que utiliza Designer, seleccione Examinar, Universos de CA.

5. Verifique la ruta de archivo para la carpeta de importación en el cuadro correspondiente.
6. Haga clic en OK.
Aparecerá la ventana Universo.

7. Seleccione Archivo, Parámetros.
Aparecerá el cuadro de diálogo Universe Parameters.
8. En la ficha Definición, haga clic en Editar.
Aparecerá el cuadro de diálogo Parámetros de inicio de sesión.
9. Seleccione las credenciales de base de datos de uso asociadas con la casilla de verificación de la cuenta de usuario de BusinessObjects.
10. Haga clic en Next, Test Connection y recorra el diálogo de conexión del universo que aparece.
11. Haga clic en Aceptar para finalizar.
12. Seleccione Archivo, Exportar.
Aparecerá el cuadro de diálogo Exportar universo.
13. Seleccione el universo que desea utilizar en la lista desplegable Dominio.
14. Seleccione Everyone de la lista Groups
15. Haga clic en OK para exportar los cambios del universo.

Establecimiento de particiones de datos

En Gestión de roles y seguridad, cree una restricción de partición de datos que limitará el acceso a los registros de la base de datos de todos los usuarios de informes asignados a la partición de datos.

Nota: Para obtener información sobre el establecimiento de restricciones en las particiones de datos, consulte Configuración de particiones de datos (see page 188).

Base de datos replicada para la generación de informes sin conexión

Para gestionar incidencias de rendimiento potenciales que pueden afectar a los componentes de la generación de informes instalados con CA Service Desk Manager, puede crear una base de datos replicada con fines de generación de informes sin conexión.

Nota: Si desea obtener más información sobre cómo crear bases de datos replicadas para la generación de informes sin conexión, consulte los scripts y la documentación de muestra que se encuentran en el directorio NX_ROOT\samples\reporting.

Informes de Role-Based

CA Service Desk Manager presenta los informes basados en roles en dos marcos de generación de informes en la ficha Informes. Cada marco proporciona vistas gráficas que permiten a los usuarios realizar búsquedas detalladas de datos de informes para mostrarlos debajo de diagramas y grupos resumidos. Puede gestionar los informes basados en roles y mostrar los informes nuevos de BusinessObjects en la ficha Informes.

La página Lista de informes contiene detalles de los informes que están disponibles para utilizarse. Haga clic en el icono de la lista de informes que aparece en el marco seleccionado para mostrar esta página.

Definición de informes de Role-Based

Puede gestionar los formularios Web de informes que aparecen en la página Lista de informes cuando un usuario asignado a este rol se conecta al sistema.

Para definir un informe de role-based para el rol

1. En la ficha Administración, vaya a Gestión de roles y seguridad, Gestión de roles, Lista de roles.

Aparecerá la página Lista de roles. Para la generación de informes se dispone de los siguientes roles predeterminados:

- Gestor de cambios
- Gestor de servicio al cliente
- Gestor de conocimientos
- Analista de conocimiento
- Service Desk Manager
- Gestor de incidentes
- Gestor de problemas

2. Seleccione de la lista *uno* de los roles de generación de informes.

Aparecerá la página de formulario Detalles del rol. Esta página contiene las siguientes fichas:

Autorización

Le permite definir el nivel de autorización asignado al rol.

Acceso a función

Le permite definir el acceso del rol a cada área funcional de CA Service Desk Manager.

Interfaz Web

Le permite personalizar la interfaz Web del rol definiendo las páginas Web y el contenido de la ayuda en línea a los que pueden acceder los usuarios.

Gestión del conocimiento

Permite especificar los privilegios de Gestión del conocimiento para el rol

Visibilidad de documento de KT

Le permite especificar qué estados de documento puede ver el rol (por ejemplo, borrador, retirado y publicado).

Fichas

Le permite definir las fichas que aparecen cuando un usuario asignado a este rol se conecta a CA Service Desk Manager.

Formularios Web

Le permite definir los formularios Web de informe a disposición de este rol.

Ir a Recursos

Le permite especificar qué tipos de registro aparecen en la lista desplegable "Ir" del rol. En la página Detalles de rol, seleccione la ficha Formularios Web de informes.

3. Haga clic en la ficha Formularios Web de informes.

Aparecerá la página Lista de formularios Web. Esta página contiene detalles de los informes que se pueden usar.

4. Haga clic en Actualizar formularios Web.

Aparecerá la página Búsqueda de formularios Web.

5. Introduzca los criterios de búsqueda para mostrar los formularios Web y haga clic en Buscar.

Aparecerá la página Actualización de formularios Web asignados mostrando una lista de los formularios que coinciden con los criterios de búsqueda introducidos.

6. En la lista de la izquierda, seleccione los formularios Web que desee mostrar para este rol. Para seleccionar varios elementos, mantenga pulsada la tecla Ctrl mientras hace clic con el botón izquierdo del ratón.

7. Cuando haya seleccionado todos los formularios que desee, haga clic en el botón Seleccionar.

Los formularios seleccionados pasan a la lista de formularios Web asignados de la derecha.

8. Haga clic en OK.

Aparecerá la página Detalles del rol, con los formularios Web seleccionados incluidos en la ficha Formularios Web.

Mostrar nuevos informes en la ficha Informes

Cuando se aprueba el uso de un informe en CA Service Desk Manager, se mueve a la sección pública de InfoView, de modo que quede disponible para usuarios autorizados. Para agregar el informe a CA Service Desk Manager, el administrador debe ejecutar algunos pasos adicionales.

Se pueden mostrar los nuevos informes creados en CA Business Intelligence en la ficha Informes de CA Service Desk Manager. Para dicha tarea, utilice las siguientes herramientas:

- Web Screen Painter
- Administración de funciones

Antes de empezar, haga lo siguiente:

- Instale y configure CA Business Intelligence de forma que funcione con CA Service Desk Manager.

Nota: Para obtener información sobre la instalación, consulte la *Guía de implementación* y la *Guía de instalación de CA Business Intelligence*.

- Permisos de usuario, roles y opciones de autenticación (see page 714) establecidos para el entorno de generación de informes.

Más información:

[Paso 1: creación de dos registros de formulario Web para llamar a los nuevos informes](#) (en la página 728)

[Paso 2: creación de una página de varios marcos y asignación de los nuevos informes](#) (en la página 729)

[Paso 3: creación de una página de inicio para la ficha Informes](#) (en la página 730)

[Paso 4: creación de un registro de la ficha Informes y asignación de la página de inicio](#) (en la página 731)

[Paso 5: asignación del registro de fichas a un registro de rol](#) (en la página 732)

[Paso 6: creación de una página de inicio para el botón InfoView](#) (en la página 733)

[Paso 7: asignación de la página de inicio del botón InfoView al registro de la ficha Informes](#) (en la página 734)

Paso 1: creación de dos registros de formulario Web para llamar a los nuevos informes

De forma predeterminada, la ficha Informes contiene dos marcos de generación de informes que permiten a los usuarios autorizados mostrar los nuevos informes. En este paso, creará dos registros de formularios Web y definirá las URL que hacen referencia a los nuevos informes.

Procedimiento para crear dos registros de formularios Web para llamar a los nuevos informes

1. En la ficha Administración, vaya a Gestión de roles y seguridad, Gestión de roles, Formularios Web.

Aparecerá la página Lista de formularios Web.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nuevo formulario Web.

3. Rellene los siguientes campos:

Nombre del formulario Web

Especifique un nombre que identifica el formulario Web. Se trata de un campo obligatorio.

Ejemplo: Informe de lista de activos

Estado de registro

Especifique activo.

Código

Especifique un valor de código exclusivo que identifica el formulario Web en el sistema. Una vez que se ha definido, este código no puede cambiarse.

Ejemplo: lista_activos

Nota: Anote el valor que escribe en el campo Código.

Tipo

Seleccione Informe.

Descripción

(Opcional) Especifique una descripción breve del formulario Web.

Recurso

Especifique la URL que llama al nuevo informe.

Ejemplo: abrir el formulario Web Lista de activos de la lista de formularios Web en Gestión de roles y especificar la URL que aparece en este formulario.

```
$BOServerURL?sPath=[Home],[Public+Folders],[CA+Reports],[CA+Service+Desk]  
,[Asset]&sDocName=Asset+List&sviewer=html
```


4. Haga clic en Guardar.
Se guardará la definición del formulario Web y aparecerá la página Detalles del formulario Web.
5. Repita los pasos 1-3 para crear un segundo registro de formulario Web que llamará a la segunda URL del informe. Anote el valor escrito en el campo Código.

Paso 2: creación de una página de varios marcos y asignación de los nuevos informes

En Web Screen Painter, cree una página de varios marcos con dos marcos verticales denominada conjunto de marcos. A continuación, asigne los registros del formulario Web creados en el paso 1 a este conjunto de marcos.

Nota: Esta página se puede crear con cualquier número de marcos. Tenga en cuenta que agregar marcos adicionales limitará la visibilidad en la ficha Informes.

Procedimiento para crear una página de varios marcos y asignar los informes

1. En Web Screen Painter, seleccione Archivo, Nuevo.
Aparecerá el cuadro de diálogo Nuevo formulario.
2. Rellene los campos de la interfaz y del grupo de formularios de la manera adecuada.
3. Seleccione multiframe.template de la lista de nombres de archivos.
4. Haga clic en Nuevo.
Aparece la ventana multiframe.html.
5. Seleccione Controles, Insertar conjunto de marcos.
Se mostrará el cuadro de diálogo Insertar conjunto de marcos.
6. No cambie la configuración predeterminada y haga clic en Aceptar.
Aparecen dos marcos verticales en el conjunto de marcos.
7. Haga clic con el botón secundario en el marco vertical de la izquierda y seleccione Propiedades en el menú contextual.
Se mostrará el cuadro de diálogo Propiedades: Conjunto de marcos.
8. Seleccione el siguiente campo en blanco situado junto al atributo web_form_name y, a continuación, haga clic en el botón (...).
Se mostrará el cuadro de diálogo Introducir nombre del formulario Web.
9. Especifique el valor de código del primer informe.

Ejemplo: lista_activos

10. Después de que encuentre el nombre del formulario Web del informe, haga clic en Validar.
11. Haga clic con el botón secundario en el marco vertical de la derecha, especifique el valor de código del segundo informe y, a continuación, valide el informe.
12. Guarde la página multiframe.html. Anote este nombre de archivo.

Ejemplo: report_mframe.html

13. Seleccione Archivo, Publicar.

La publicación pone el formulario a disposición de todos los usuarios de CA Service Desk Manager. Para el rol de analista, el archivo está disponible en la siguiente ubicación: Archivos de programa/CA/Service Desk/Site/mods/www/html/web/analyst/report_mframe.html.

Nota: Cuando busque formularios Web de varios marcos en CA Service Desk Manager, vaya a Gestión de roles y seguridad, Gestión de roles, Formularios Web en la ficha Administración. La columna Código especifica el web_form_name en la ficha Propiedades correspondiente a un formulario de varios marcos en Web Screen Painter.

Paso 3: creación de una página de inicio para la ficha Informes

En Gestión de roles, cree una página de inicio para llamar a la página Web de varios marcos creada en el paso 2.

Para crear una página de inicio para la ficha Informes

1. En la ficha Administración, vaya a Gestión de roles y seguridad, Gestión de roles, Formularios Web.

Aparecerá la página Lista de formularios Web.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nuevo formulario Web.

3. Rellene los siguientes campos:

Nombre del formulario Web

Especifique un nombre que identifica el formulario Web. Este campo es obligatorio.

Ejemplo: página de inicio

Estado de registro

Especifique activo o inactivo.

Código

Especifique un valor de código exclusivo que identifica el formulario Web en el sistema. Una vez definido, este código no puede cambiarse.

Ejemplo: start_page

Tipo

Especifique HTML.

Descripción

(Opcional) Especifique una descripción breve del formulario Web.

Recurso

Especifica la URL que llama al nuevo informe.

Por ejemplo: seleccione del registro Informes de administrador multimarco de la página Lista de formularios Web. Especifique la URL que aparece en este formulario. Al final de esta ruta, especifique la nueva página de varios marcos (report_mframe.html).

`$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=report_mframe.html`

Haga clic en Guardar.

Aparece el nuevo registro de página de inicio en la página Lista de formularios Web.

Paso 4: creación de un registro de la ficha Informes y asignación de la página de inicio

En Gestión de roles, cree una nueva ficha Informes y especifique la página de inicio creada en el paso 3.

Para crear una ficha y asignar la página de inicio que llama a los informes

1. Seleccione Gestión de roles y seguridad, Gestión de roles, Fichas en la ficha Administración.

Aparecerá la página Lista de ficha.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nueva ficha.

3. Rellene los siguientes campos:

Nombre de la ficha

Especifique el nombre que identifica la ficha en la interfaz de administración. Por ejemplo, el nombre de la ficha aparece en la página Lista de fichas.

Por ejemplo: ficha Informes

Código

Especifique el código que identifica esta ficha en el sistema. Una vez que se ha definido, este código no puede cambiarse.

Ejemplo: reports_tab

Estado de registro

Especifique activo.

Visualizar nombre

Especifique el nombre que aparece en la presentación gráfica de la ficha en la interfaz de usuario.

Por ejemplo: ficha Informes

Página de inicio

Especifique el formulario Web inicial que aparece en la ventana principal cuando un usuario selecciona esta ficha.

Ejemplo: página de inicio

4. Haga clic en Guardar.

Aparece el formulario en la página Lista de formularios Web.

Paso 5: asignación del registro de fichas a un registro de rol

En Gestión de roles, asigne la ficha Informes al rol de la lista que aparece en la página Detalles del rol que desee. Cuando un usuario asignado a este rol se conecte al sistema, verá en la interfaz Web la nueva ficha Informes.

Para asignar el registro de ficha a un registro de rol

1. Seleccione Gestión de roles y seguridad, Gestión de roles, Lista de roles en la ficha Administración.

Aparecerá la página Lista de roles.

2. Seleccione el rol deseado en la lista de roles.

Aparecerá la página Detalles del rol.

3. En el final de esta página, seleccione Fichas y, a continuación, Actualizar fichas.

Aparece la nueva ficha en la lista de fichas.

Paso 6: creación de una página de inicio para el botón InfoView

Tiene la opción de incluir el botón InfoView que abre BusinessObjects InfoView en una nueva ventana en la ficha Informes. Esta opción se controla a través de la opción Página de inicio que aparece en el registro de la ficha Informes.

Procedimiento para crear una página de inicio para el botón InfoView

1. En la ficha Administración, vaya a Gestión de roles y seguridad, Gestión de roles, Formularios Web.

Aparecerá la página Lista de formularios Web.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nuevo formulario Web.

3. Rellene los siguientes campos:

Nombre del formulario Web

(Requerido) Especifique un nombre que identifica el formulario Web.

Por ejemplo: página InfoView

Estado de registro

Especifique activo o inactivo.

Código

(Requerido) Especifique un valor de código que identifica el formulario Web en el sistema.

Ejemplo: info_view_page

Tipo

Especifique HTML.

Descripción

(Opcional) Describa el formulario Web.

Recurso

Especifique la URL que llama a los marcos de generación de informes.

Ejemplo: seleccione el registro InfoView del administrador en la página Lista de formularios Web. Especifique la URL que aparece en este formulario. Al final de esta ruta, especifique la nueva página de inicio de la ficha Informes (página_inicio).

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=show_report_frames.html+KEEP.report_form=página_inicio
```

Haga clic en Guardar.

Aparece la página de inicio de InfoView en la página Lista de formularios Web.

Paso 7: asignación de la página de inicio del botón InfoView al registro de la ficha Informes

En Gestión de roles, asigne la página de inicio del botón InfoView creada en el paso 6 al registro de la ficha Informes.

Procedimiento para asignar la página de inicio del botón InfoView al registro de la ficha Informes

1. Seleccione el nuevo registro de formulario Web de la ficha Informes desde la página Lista de fichas en Gestión de roles.

Aparecerá la página de detalles.

2. Seleccione Editar.

Aparecerá la página Actualizar ficha.

3. Especifique la nueva página de inicio del botón InfoView en el campo Página de inicio.

4. Haga clic en Guardar.

Cuando un usuario abre la ficha Informes, el botón InfoView aparece en la esquina superior derecha del formulario.

Informes basados en Web

CA Business Intelligence instala un conjunto de informes predefinidos basados en Web para CA Service Desk Manager y Gestión del conocimiento. Éstos se desarrollan mediante BusinessObjects Enterprise Web Intelligence o Crystal Reports. Los informes se pueden utilizar como modelos para definir los informes específicos del sitio.

Estos informes se encuentran en carpetas que se implementan automáticamente en el servidor de informes de CA Business Intelligence después de la instalación.

Se puede asignar seguridad a carpetas y documentos para especificar si permiten un acceso global, un acceso de roles específicos o de individuos.

Nota: Para obtener información general sobre el uso de informes predefinidos, consulte la *Ayuda en línea*. También consulte la *Guía del usuario de BusinessObjects InfoView*.

Más información:

[Interfaz de BusinessObjects InfoView](#) (en la página 735)

[Desplazamiento por los informes](#) (en la página 735)

[Preferencias de InfoView](#) (en la página 736)

[Programación de informes](#) (en la página 736)

[Configuración de análisis de datos](#) (en la página 737)

[Publicación y distribución de informes](#) (en la página 737)

Interfaz de BusinessObjects InfoView

En la ficha Informes de CA Service Desk Manager, los analistas y los gestores pueden trabajar con los informes definidos para su rol o gestionar informes personales al hacer clic en el botón InfoView. En InfoView, los usuarios pueden acceder a los informes de Crystal Reports y los documentos de Web Intelligence y otros objetos, y organizarlos en función de sus preferencias.

Las funciones que están disponibles en InfoView varían según el tipo de contenido, pero, en general, el usuario puede ver la información en el explorador Web, exportarla a otras aplicaciones empresariales (como Microsoft Excel) y guardarla en una ubicación especificada.

Nota: Las carpetas y los objetos que los usuarios pueden ver en InfoView dependen de la asignación de grupo (rol).

Desplazamiento por los informes

Puede desplazarse por los informes del panel izquierdo de la ventana InfoView para ver, programar, modificar o ejecutar los informes o para ver su historial y propiedades.

Procedimiento para ver un informe

1. Utilice *uno* los métodos siguientes para abrir InfoView:
 - En la ficha Informes de CA Service Desk Manager, haga clic en el botón InfoView.
 - En el menú Inicio, vaya a BusinessObjects XI Release2, BusinessObjects Enterprise, BusinessObjects Enterprise Java InfoView.

Aparecerá la página inicial de InfoView.
2. En el panel izquierdo, desplácese por la estructura de carpetas Public Folders/CA Reports/CA Service Desk Manager.
3. Haga clic en la carpeta que corresponde al tipo de informe que desea ver.

4. Haga clic en el nombre del informe para el tipo de información que desea consultar.

El informe aparece en BusinessObjects InfoView.

Nota: Para obtener más información sobre cómo definir preferencias y utilizar informes, consulte la *Guía del usuario de BusinessObjects InfoView*.

Preferencias de InfoView

Los usuarios pueden establecer preferencias generales para especificar que InfoView se inicie con una de las páginas del escritorio personales diseñadas mediante la herramienta My InfoView de Web Intelligence. También pueden establecer preferencias personales de visualización de Web Intelligence y Crystal Reports.

Nota: Para obtener más información sobre cómo definir preferencias, consulte la *Guía del usuario de BusinessObjects InfoView*.

Programación de informes

InfoView admite la programación de informes. Para la generación de informes ad hoc, los informes programados se almacenan en la sección Mis carpetas. Si un informe se establece en "actualizar al abrir" el sistema tendrá acceso a la base de datos para obtener la información más reciente cada vez que el usuario final vea el informe. Los usuarios pueden programar los informes para que se ejecuten en determinados momentos.

Los administradores pueden definir calendarios que reflejen fechas de programación adecuadas. Por ejemplo, un usuario puede seleccionar un calendario utilizando la opción "Cuando" (para el tiempo y la frecuencia) que mostrará los días hábiles disponibles e ignorará los días no laborables.

Nota: Para obtener más información sobre la programación de informes, consulte la documentación de BusinessObjects.

Mediante la programación, los usuarios pueden:

- Especificar el tiempo y frecuencia de la programación (por ejemplo: ahora, por horas, diario y semanal).
- Especifique el destino, como por ejemplo la bandeja de entrada, la ubicación del archivo o el destinatario de correo electrónico.
- Indique a qué bandejas de entrada se debe enviar el informe.
- Especifique la salida, por ejemplo Web Intelligence, Crystal Reports, Microsoft Excel y Adobe Acrobat.

- Especifique las opciones de almacenamiento en caché. De forma predeterminada, los resultados del documento se almacenan en el servidor de repositorio de archivos de salida. Los usuarios pueden determinar que el sistema almacene el informe en caché en el servidor de informes de Web Intelligence seleccionando un formato de caché y una configuración local.
- Seleccione un grupo de servidores para procesar la solicitud. Si se selecciona un evento definido, el objeto se ejecutará solamente cuando se produzca la condición o el evento adicional.

Nota: Si se utilizan particiones de datos de CA Service Desk Manager para gestionar restricciones de datos en la sección de carpetas públicas de InfoView, los informes programados contenidos en las carpetas públicas se deben definir para cada usuario.

Configuración de análisis de datos

Un visor interactivo que ofrece un amplio conjunto de herramientas para ajustar la forma de visualización de los datos de informes. Se pueden realizar búsquedas con diversos niveles de detalle, por ejemplo, del grupo, al asignatario o a las solicitudes reales.

Los visores interactivos permiten hacer lo siguiente:

- Cambie el aspecto del informe presentando los datos en un formato de "bloque" diferente, como un gráfico circular. Por ejemplo, al hacer clic con el botón derecho en el informe y seleccionar "Turn table to", aparecen funciones de presentación de informes.
- Realice diferentes tareas, como la ordenación, creación de divisiones, cálculo, filtrado y clasificación del informe.
- Comparta información con otros usuarios y grupos.

Nota: Para obtener más información acerca del análisis de datos, consulte la *Guía del usuario de BusinessObjects InfoView*.

Publicación y distribución de informes

Los usuarios de InfoView pueden guardar datos de informes en formato Excel, PDF o CSV y, a continuación, distribuirlos a una ubicación de archivos, la bandeja de entrada, una dirección de correo electrónico o un sitio FTP.

Cuando se aprueba el uso de un informe en CA Service Desk Manager, éste se traslada a la sección pública de forma que queda disponible para usuarios autorizados. Se puede asignar seguridad a carpetas y documentos para especificar si permiten un acceso global, un acceso de roles específicos o de individuos. La seguridad se administra en la consola de gestión central de BusinessObjects.

Nota: Para obtener información sobre cómo publicar y distribuir informes, consulte la *Guía del usuario de BusinessObjects InfoView*.

Informes de cuadros de mandos

Puede utilizar la generación de informes del cuadro de mandos para controlar las operaciones diarias de todos los tipos de ticket de CA Service Desk Manager (solicitud/incidente/problema, orden de cambio o incidencia) en BusinessObjects InfoView. Cada informe contiene un análisis sobre los principales realizadores que trabajan en tickets activos, de modo que sea posible controlar su progreso. Con la generación de informes de cuadros de mandos, se puede:

- Visualizar información detallada y de resumen sobre los tickets activos por prioridad, analista, categoría o grupo.
- Descubrir cuántos tickets han sido resueltos en un período de tiempo determinado y mucho más.
- Editar, imprimir, realizar el seguimiento y guardar informes en otros formatos, como .xls y .pdf.

Puede trabajar por separado con informes de cuadros de mandos predefinidos o utilizar el cuadro de mandos corporativo para ver todas las operaciones diarias de CA Service Desk Manager en una sola vista. El cuadro de mandos corporativo comparte información vital sobre las operaciones diarias para todos los tipos de ticket (solicitud/incidente/problema, orden de cambio o solicitud) por prioridad, analista, categoría o grupo.

Nota: Al trabajar con la generación de informes del cuadro de mandos, puede utilizar las características de InfoView descritas en la sección Operaciones con cuadro de mandos y análisis de la *Guía del usuario de BusinessObjects Enterprise InfoView*.

Visualización de informes de cuadros de mandos operativos

Los usuarios autorizados pueden visualizar los informes predefinidos de cuadro de mandos en BusinessObjects InfoView. Las carpetas y los informes que se pueden ver en InfoView dependen de la cuenta con la que se inicia sesión y los derechos que le ha concedido el administrador.

Nota: Para obtener información de inicio de sesión, póngase en contacto con su administrador.

Procedimiento para visualizar un informe de cuadros de mandos operativos

1. En la ficha Informes de CA Service Desk Manager, haga clic en el botón InfoView e inicie sesión en InfoView con sus credenciales.
InfoView aparece en su explorador Web.
2. En la barra de herramientas de InfoView, seleccione Cuadros de mandos, Cuadros de mandos corporativos, Operaciones diarias del gestor del Centro de servicio al usuario.
Las carpetas y los objetos aparecen en el área de navegación.
3. Seleccione Carpetas públicas, Informes de CA, Cuadro de mandos operativo.
Aparecen las siguientes carpetas: Orden de cambio, Incidente, Incidencia, Problema, Solicitud.
4. Seleccione el informe adecuado.
El informe de cuadro de mandos aparece en el panel derecho.
5. Haga clic en doble el título para mostrar un informe.
El informe se abre para la visualización.

Informes ad hoc

Los informes ad hoc se desarrollan en InfoView utilizando Web Intelligence. Puede crear informes ad hoc.

Nota: Para obtener más información sobre informes ad hoc, consulte la documentación de BusinessObjects Enterprise.

Interfaz de Web Intelligence

En InfoView, Web Intelligence ofrece una herramienta de generación de informes personalizados que se ha diseñado para los usuarios que desean crear informes básicos de forma sencilla, sin necesidad de escribir consultas. Web Intelligence utiliza modelos y plantillas de informes predefinidos que gestionan conexiones de datos, consultas y relaciones de datos, de manera que solamente necesite arrastrar y soltar campos de datos en una plantilla para crear informes tabulares o de matriz. Puede utilizar todas las funciones de InfoView descritas en la *guía del usuario de InfoView*.

Un documento de Web Intelligence hace referencia a un objeto de BusinessObjects denominado universo para crear informes. Los informes nuevos se crean en universos de BusinessObjects. CA Business Intelligence proporciona el universo de CA Service Desk Manager con el producto.

Cómo funcionan los informes ad hoc

Los informes ad hoc funcionan del siguiente modo:

1. Inicie el informe ad hoc seleccionando primero el universo de CA Service Desk Manager en InfoView.
2. El universo se asigna a la base de datos de CA Service Desk Manager que contiene información empresarial corporativa. Cuando se conecta a un universo, Web Intelligence inicia automáticamente el editor de documentos seleccionado en la página Preferencias de documento de Web Intelligence de InfoView.

Nota: Para obtener más información sobre cómo definir preferencias, consulte la *Guía del usuario de InfoView*.

3. Utilizando el universo, puede crear consultas para recuperar datos que se utilizan en un informe de objetos agrupados en carpetas denominadas clases. Cada clase puede contener también una o varias subclases. Las subclases contienen objetos que son una subcategoría adicional de los objetos del nivel superior de la clase. Las clases y los objetos se presentan en una estructura de árbol (jerarquía) en la ficha Datos.

Nota: Para obtener instrucciones sobre cómo crear consultas para documentos de Web Intelligence, consulte la documentación de BusinessObjects Enterprise.

4. Después de crear la consulta, agregando los objetos necesarios al panel Objetos de resultado y las propiedades de filtrado de consulta definidas, está preparado para ejecutarla. Al ejecutar una consulta, el universo pide a la base de datos que recupere los datos que corresponden a las demandas de cada uno de los objetos de la consulta. Puede ejecutar una consulta haciendo clic en Ejecutar consultas en la barra de herramientas.

Importante: Al seleccionar los objetos para la consulta, elija siempre objetos, medidas y filtros sólo de una clase básica del universo y sus subclases. Si incluye objetos, medidas y filtros de múltiples clases básicas de universo en una consulta, podría provocar resultados inesperados y un rendimiento bajo.

Informes ad hoc de ejemplo

Puede trabajar con ejemplos de consulta y Web Intelligence y crear informes ad hoc que utilicen el universo predeterminado de CA Service Desk Manager. Cuando cree un informe, asegúrese de guardarlo con regularidad. Si se supera el tiempo de espera de la sesión de conexión de Web Intelligence, perderá las modificaciones realizadas en el informe.

Nota: Para obtener información sobre cómo cambiar el valor de tiempo de espera de la sesión, consulte la *Guía de implementación*.

Más información:

[Ejemplo: Visualización de todas las solicitudes de prioridad 1 y 2 abiertas para todos los usuarios](#) (en la página 741)

[Ejemplo: Visualización de todas las solicitudes abiertas que no incluyan el estado Trabajo en curso](#) (en la página 743)

[Ejemplo: Visualización de todas las solicitudes cerradas en los últimos 30 días de los usuarios cuyo apellido comience por "C"](#) (en la página 745)

Ejemplo: Visualización de todas las solicitudes de prioridad 1 y 2 abiertas para todos los usuarios

En este ejemplo, especificará los valores de mensajes que reunirán los datos adicionales antes de la generación del informe.

Ejemplo: Visualización de todas las solicitudes de prioridad 1 y 2 abiertas para todos los usuarios

1. Haga clic en Nuevo, Documento de Web Intelligence en la barra de menús. Aparecerá la página Nuevo documento de Web Intelligence.

2. Seleccione el universo de CA Service Desk Manager en la columna Universo.

El documento de Web Intelligence aparece junto a la información del universo en el panel izquierdo.

Nota: Para mejorar la navegación, cierre la carpeta Tipo de servicio adjunto en el panel de la izquierda.

3. Localice y, a continuación, expanda las carpetas de Solicitud, Detalles de la solicitud del panel izquierdo. Utilice la barra de desplazamiento para buscar las carpetas.
4. Seleccione cada uno de los siguientes objetos y, a continuación, arrástrelos y suéltelos del panel de la izquierda al de la parte superior derecha situado debajo de los objetos de resultado.
 - Resumen
 - Símbolo de prioridad
 - Nombre combinado de cliente
5. Seleccione los objetos siguientes, y arrástrelos y suéltelos en el panel inferior derecho situado debajo de Filtros de consulta. Cuando termine, cierre la carpeta Detalles de la solicitud.
 - Símbolo de estado
 - Símbolo de prioridad
6. Amplíe la carpeta Filtros de solicitudes y, a continuación, arrastre y suelte el Nombre combinado de cliente con el filtro Userid al panel inferior derecho situado debajo de Filtros de consulta.
7. En el panel Filtros de consulta, haga clic en la flecha de En lista en el objeto Símbolo de estado, y seleccione el operador Igual a.
8. Seleccione valores de la lista del menú Operand Type.

Aparecerá el cuadro de diálogo Lista de valores.
9. En la lista Símbolo de estado, seleccione Abierto y, a continuación, haga clic en la flecha verde.

El valor aparece en el campo Valores seleccionados.
10. Haga clic en OK.
11. En el panel Filtros de consulta, haga clic en la lista desplegable en el filtro Símbolo de prioridad, y seleccione el operador En lista.
12. En la lista Símbolo de prioridad, realice la selección múltiple 1 y 2 y, a continuación, haga clic en la flecha verde.

Los valores 1 y 2 aparecen en el campo Valores seleccionados.
13. Haga clic en OK.

14. Haga clic en Ejecutar consulta en la barra de herramientas para generar el informe.

Nota: Como el Nombre combinado de cliente con el filtro rápido Userid utiliza la función Mensaje, aparece el cuadro de diálogo Mensaje. Este diálogo permite reunir más datos antes de que se genere el informe.

15. En la ventana Mensajes, seleccione la primera opción TODOS y, a continuación, haga clic en el botón de la flecha verde.

Aparecen todos los nombres de usuario en la lista Seleccionar cliente.

16. Haga clic en Ejecutar consulta para generar el informe.

Aparecerá el informe en una nueva ventana.

17. Haga doble clic en el título del informe y escriba Solicitudes abiertas de prioridad 1 y 2 para todos los usuarios en el cuadro de texto. Puede cambiar el tamaño de fuente a 16 u otros tamaños.

18. Para cambiar otros aspectos del informe, haga clic en la ficha Propiedades.

19. Para subagrupar los datos por Apellido del cliente, haga clic con el botón derecho en cualquier celda de datos en la columna Apellido del cliente, y seleccione Definir como sección.

20. Haga clic en Guardar y especifique una ubicación mediante la opción Guardar como.

Ejemplo: Visualización de todas las solicitudes abiertas que no incluyan el estado Trabajo en curso

En este ejemplo, especificaré la función de generación de informes Número para devolver el número total de solicitudes abiertas.

Ejemplo: Visualización de todas las solicitudes abiertas que no tengan el estado Trabajo en curso

1. Haga clic en Nuevo, Documento de Web Intelligence en la barra de menús.

Aparecerá la página Nuevo documento de Web Intelligence.

2. Seleccione el universo de CA Service Desk Manager en la columna Universo.

El documento de Web Intelligence aparece junto a la información del universo en el panel izquierdo.

Nota: Para mejorar la navegación, cierre la carpeta Tipo de servicio adjunto en el panel de la izquierda.

3. Localice y, a continuación, expanda las carpetas de Solicitud, Detalles de la solicitud del panel izquierdo. (Utilice la barra de desplazamiento para desplazarse por las carpetas).

4. Seleccione cada uno de los siguientes objetos y, a continuación, arrástrelos y suéltelos del panel de la izquierda al de la parte superior derecha situado debajo de los objetos de resultado.
 - Símbolo de estado
 - Núm. referencia
 - Resumen
5. Seleccione el objeto Símbolo de estado y arrástrelo al panel inferior derecho situado debajo de Filtros de consulta. Cierre la carpeta Detalles de la solicitud.
6. Amplíe la carpeta Filtros de solicitudes y, a continuación, arrastre y suelte el filtro Activo al panel inferior derecho situado debajo de Filtros de consulta.
7. En el panel Filtros de consulta, haga clic en la flecha de En lista en el objeto Símbolo de estado, y seleccione el operador No igual a.
8. Seleccione Trabajo en curso en el menú Operand Type.
9. Haga clic en Editar Informe en la barra de herramientas principal.
Se abrirá el visor de informes.
10. En el informe, seleccione la columna Núm. referencia. Esta acción habilita el comando Insertar suma en la barra de herramientas Generación de informes.
11. Haga clic en el comando Insertar suma y, a continuación, seleccione Recuento del menú.
12. En el informe, haga clic con el botón derecho en la celda =[Símbolo de estado] y seleccione Definir como sección en el menú contextual.
13. Haga clic en Actualizar datos en la barra de herramientas principal para ejecutar el informe.
14. Haga clic en Guardar.

El informe muestra el número total (recuento) de solicitudes que *no* tienen un estado de Trabajo en curso.

Ejemplo: Visualización de todas las solicitudes cerradas en los últimos 30 días de los usuarios cuyo apellido comience por "C"

En este ejemplo, especificará valores de mensaje para los objetos Fecha de cierre y Apellido del cliente que devolverán todas las solicitudes cerradas basadas en estos valores.

Ejemplo: Visualización de todas las solicitudes cerradas de los últimos 30 días de los usuarios cuyo apellido comience por "C"

1. Haga clic en Nuevo, Documento de Web Intelligence en la barra de menús.
Aparecerá la página Nuevo documento de Web Intelligence.
2. Seleccione el universo de CA Service Desk Manager en la columna Universo.

El documento de Web Intelligence aparece junto a la información del universo en el panel izquierdo.

Nota: Para mejorar la navegación, cierre la carpeta Tipo de servicio adjunto en el panel de la izquierda.
3. Localice y expanda las carpetas Solicitud, Detalles de la solicitud del panel izquierdo. Utilice la barra de desplazamiento para desplazarse por las carpetas.
4. Seleccione cada uno de los siguientes objetos y, a continuación, arrástrelos y suéltelos del panel de la izquierda al de la parte superior derecha situado debajo de los objetos de resultado.
 - Núm. referencia
 - Fecha de cierre
 - Apellidos del cliente
 - Resumen
5. Seleccione cada uno de los objetos siguientes, y arrástrelos al panel inferior derecho situado debajo de Filtros de consulta.
 - Símbolo de estado
 - Fecha de cierre
 - Apellidos del cliente
6. Haga clic en la flecha En lista del filtro de Símbolo de estado y seleccione valores de la lista del menú Operand Type.

Aparecerá el cuadro de diálogo Lista de valores.
7. Seleccione los valores siguientes en la lista Símbolo de estado:
 - Closed (Cerrado)
 - Cerrado - Sin resolver

- Cierre solicitado
- Problema - Cerrado
- Problema - Corregido
- Resuelto

8. Haga clic en la flecha verde.

Los valores aparecen en el campo Valores seleccionados.

9. Haga clic en OK.

10. En el panel Filtros de Consulta, haga clic en la flecha de En lista en el objeto Fecha de cierre y seleccione el operador Entre.

11. Haga clic en la flecha de En lista y seleccione Mensaje en el primer y segundo menú Operand Type.

12. Haga clic en la flecha de En lista del objeto Apellido del cliente y seleccione el operador Matches pattern.

13. Haga clic en la flecha de En lista y seleccione Mensaje del menú Operand Type.

14. Haga clic en el icono Propiedades de mensaje que aparece junto a la flecha de En lista.

Aparecerá el cuadro de diálogo Mensaje.

15. En el campo de texto de Mensaje, escriba un patrón para Apellido del cliente.

16. Haga clic en OK.

17. Haga clic en Ejecutar consulta en la barra de herramientas para generar el informe.

Nota: Como los objetos Fecha de cierre y Apellido del cliente utilizan la función Mensaje, aparece el cuadro de diálogo Mensajes. Este diálogo permite reunir más datos antes de que se genere el informe.

18. En la ventana Mensajes, seleccione o escriba los valores de mensaje para cada mensaje, como se indica a continuación:

- Escriba la Fecha de cierre (Inicio): especifique una fecha que sea 30 días anterior a la fecha de hoy.
- Escriba la Fecha de cierre (Finalización): especifique la fecha de hoy.
- Escriba un patrón para Apellido del cliente: especifique C%.

19. Haga clic en Ejecutar consulta para generar el informe.

Aparecerá el informe en una nueva ventana.

20. Haga doble clic en el título del informe y escriba Visualización de todas las solicitudes cerradas en los últimos 30 días de los usuarios cuyos apellidos comienzan con "C" en el cuadro de texto. Puede cambiar el tamaño de fuente a 16 u otros tamaños.
21. Para cambiar otros aspectos del informe, haga clic en la ficha Propiedades.
22. Haga clic en Guardar y especifique una ubicación mediante la opción Guardar como.

Indicadores clave de rendimiento

Los *indicadores clave de rendimiento* (KPI) son medidas que el usuario puede utilizar para identificar las áreas del entorno de gestión de servicios que pueden necesitar atención administrativa o algún ajuste de configuración.

Utilice la interfaz Web de CA Service Desk Manager para configurar las definiciones de KPI. Los datos que generan se almacenan en la base de datos de CA Service Desk Manager y están disponibles para generar informes basados en Web.

Nota: Además de definir las consultas de KPI, puede configurar el daemon de KPI para recuperar datos sobre tickets de CA Service Desk Manager siempre que se abra o cierre un ticket o se modifiquen determinados campos.

Si define y controla un conjunto bien planificado de indicadores clave de rendimiento (KPI), podrá medir el avance hacia los objetivos de su organización en relación con el rendimiento, y reunir valiosos datos para tomar decisiones estratégicas acerca de su entorno de TI.

Nota: Para obtener más información sobre las tablas de bases de datos de KPI, consulte la *Guía de referencia técnica*.

KPI Types

CA Service Desk Manager proporciona tres tipos de KPI:

- Los **KPI de sistema** se instalan con el producto. No podrá crear nuevos KPI de sistema, pero los puede personalizar para adaptarlos a sus necesidades.
- Los **KPI de consultas almacenadas** llaman a una consulta almacenada para recuperar métricas de la base de datos. Puede crear KPI de consultas almacenadas personalizadas, o modificar los ejemplos predefinidos que se han instalado con el producto.

- Los **KPI SQL** permiten incorporar directamente en el KPI una consulta SQL completa. Puede crear KPI SQL personalizados, o modificar los ejemplos predefinidos instalados con el producto.

Notas:

- Para obtener detalles sobre la configuración de los tres tipos de KPI, consulte la *Ayuda en línea*.
- No se pueden suprimir los KPI, sean predefinidos o creados por el usuario. Cuando un KPI ya no se necesita, lo puede desactivar estableciendo el Estado del registro en inactivo.

KPI predefinidos

Con CA Service Desk Manager, se instalan varios KPI de cada tipo. Quizás le resulte útil examinarlos mientras lee esta guía.

Puede utilizar los KPI de consultas almacenadas y los KPI SQL con sus definiciones originales, o como modelos para definiciones personalizadas.

Puede utilizar los KPI de sistema predefinidos con las definiciones originales, o modificar algunos de los campos para adaptarlos a sus necesidades.

Nota: La mayor parte de los KPI predefinidos se establecen en un estado inactivo de forma predeterminada. Para verlos en la interfaz Web, filtre la página Lista de KPI para mostrar los KPI inactivos.

Daemon de KPI

El daemon de KPI gestiona la recuperación, organización y almacenamiento de los datos de métricas de KPI. El daemon se ejecuta continuamente, y recolecta los datos de distintos recursos del sistema en los intervalos especificados.

Cuando se alcanza el tiempo de actualización de un KPI, el daemon de KPI interactúa con otros componentes del sistema de la siguiente manera:

- **KPI de sistema:** envía una solicitud a un daemon de destino (webengine, domsrvr, bpvirtodb, o db_agents) para recuperar datos de número o duración.
- **KPI de consulta almacenada:** envía una solicitud a domsrvr para recopilar datos de número.

- **KPI SQL:** Envía una solicitud a domsrvr para recopilar datos de número, suma, máx o duración.

Cuando el daemon de KPI recibe los datos solicitados, almacena la métrica resultante en la base de datos.

Nota: La duración calculada se basa en un cambio a los valores de un ticket en tiempo real y no en horas de negocio.

KPIs de sistema

Los KPI de sistema le permiten recopilar datos de métricas relacionados con la operación de procesos de CA Service Desk Manager.

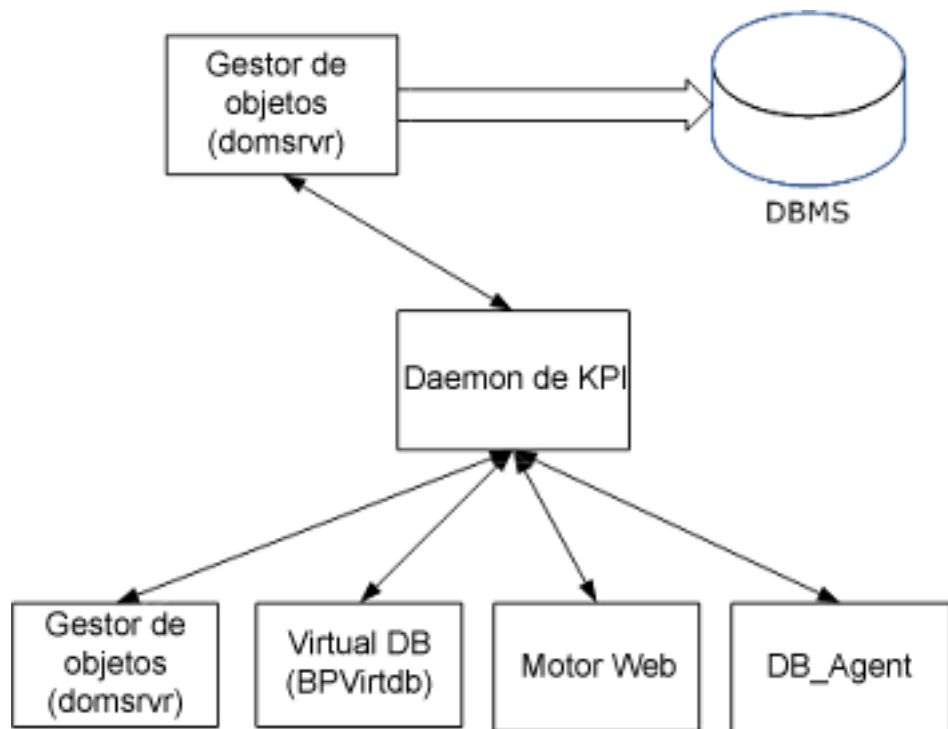
Se admiten los tipos de proceso siguientes:

- **domsrvr:** El gestor de objetos de CA Service Desk Manager (proceso del servidor). El gestor de objetos también almacena en memoria caché distintos registros y tablas para clientes.
- **bpvirtdb:** el servidor de la base de datos virtual BOP permite el funcionamiento de múltiples gestores de objetos en el entorno de CA Service Desk Manager. Todos los gestores de objetos que se ejecutan en servidores primarios o secundarios se conectan a la base de datos virtual, que arbitra su acceso a los agentes de base de datos. Por ejemplo, al recuperar un nuevo intervalo de números de referencia de tickets, la base de datos virtual garantiza que sólo un gestor de objetos a la vez tenga acceso a la tabla que contiene los números de referencia. La base de datos virtual también realiza el almacenamiento en memoria caché de la información de base de datos para los gestores de objetos.
- **db_agents:** los agentes de base de datos ejecutan consultas SQL y controlan otras interacciones entre CA Service Desk Manager y el sistema de gestión de bases de datos (DBMS). Los agentes de base de datos siguen el esquema de base de datos de CA Service Desk Manager, y traducen el código SQL al formulario requerido por el DBMS específico (por ejemplo, Oracle).

- **webengine:** El componente de CA Service Desk Manager que conecta los exploradores Web a un gestor de objetos a través de pdmweb cgi que se ejecuta en un servidor Web Microsoft IIS o Apache Tomcat. Debe haber un motor Web para WSP en el servidor primario para que el creador de esquemas de WSP pueda crear archivos de esquema. Los motores Web son los verdaderos clientes de un gestor de objetos para los exploradores Web cliente del usuario. Los motores Web almacenan en memoria caché los formularios Web .html para los usuarios conectados. Puede manipular la memoria caché mediante la utilidad pdm_webcache y ver las estadísticas de conexión del cliente mediante la utilidad pdm_webstat.

Nota: Para obtener más información sobre estos procesos, consulte la *Guía de implementación*.

El siguiente diagrama ilustra el flujo de datos de los KPI de sistema.



Cada KPI de sistema genera uno de los siguientes tipos de métrica:

- Número
- Duración

Ejemplos de KPI de sistema

- Este ejemplo genera un recuento de las solicitudes de actualización enviadas a la base de datos virtual BOP:

updateCt

- Este ejemplo informa el tiempo que las solicitudes de actualizaciones, inserciones y eliminaciones para la base de datos virtual BOP tardan en completarse:

```
virtddbupdateResponseDt
```

KPI de consultas almacenadas

Con los KPI de consultas almacenadas se puede generar informes basados en métricas de recuentos recuperadas de la base de datos de CA Service Desk Manager.

CA Service Desk Manager proporciona un conjunto de consultas almacenadas predefinidas. Muchas son útiles tal como están definidas. Además, las puede personalizar para adaptarlas a sus necesidades, o utilizarlas como modelos para escribir sus propias consultas.

Todas los KPI de consultas almacenadas tienen un tipo de métrica de Número.

Nota: Puede utilizar consultas almacenadas para producir campos de contadores para el panel de resultados de la interfaz Web, para métricas de KPI, o para ambos. Para utilizar una consulta almacenada en una definición de KPI, la consulta debe estar habilitada para el uso de KPI. Para obtener más información, consulte Configuración de consultas almacenadas (see page 351).

Ejemplos de KPI de consultas almacenadas

- Este ejemplo produce un recuento de las órdenes de cambio abiertas en la ubicación del asignatario:

```
Cambios de @cnt.location.name
```

- Este ejemplo produce un recuento de las tareas de workflow que infringirán un SLA antes de la medianoche del día actual:

```
Tareas del workflow de incidencias que hoy infringirán un SLA
```

KPI SQL

Los KPI SQL proporcionan más flexibilidad que los KPI de consulta almacenada. Con los KPI SQL puede escribir sus propias consultas a la base de datos de CA Service Desk Manager para generar los siguientes tipos de métricas:

- Sumar
- Número

- Máx.
- Duración

Nota: el código SQL debe ajustarse a la sintaxis de SQL92.

Las consideraciones siguientes se aplican a KPI SQL:

- Para ver el código SQL para estas consultas de ejemplo, abra las definiciones de las consultas de la página Lista de KPI.

Nota: Para obtener instrucciones, consulte la *Ayuda en línea*.

- El símbolo de @ no se admite en los KPI SQL. En lugar de ello, utiliza la sintaxis que se muestra en el ejemplo siguiente y un alias de atributo:

```
SELECT * FROM cr WHERE assignee_last_name = "Pérez"
```

Por ejemplo, podría utilizar un alias de atributo predefinido. Aparecerá la página Detalles de alias de atributo, de esta manera:

```
" Nombre de objeto      = cr
" Nombre de alias       = assignee_last_name
" Estado                = Activo
" Valor del alias       = assignee.last_name
```

Ejemplos: KPI de consulta SQL

- Este ejemplo predefinido genera la suma de los costes estimados de todas las tareas del workflow de órdenes de cambio pendientes:

Costes estimados de tareas del workflow de órdenes de cambio pendientes

- Este ejemplo predefinido genera un recuento de las órdenes de cambio activas cerradas y reabiertas:

Recuento de órdenes de cambio reabiertas

Campos KPI

En la siguiente tabla se describen todos los campos de KPI. Las columnas Sys. S.Q. y SQL indican los tipos de KPI a los que pertenece cada campo (sistema, consulta almacenada o SQL).

Nota: Todos los campos son necesarios a menos que se especifiquen como opcionales.

Campo	Sys.	S.Q.	SQL	Descripción
Nombre del indicador clave de rendimiento	X	X	X	Define el nombre para mostrar para el KPI. No editable.
Tipo	X	X	X	Define el registro como un sistema, consulta almacenada o KPI SQL. No editable.
Guardar versión existente	X	X	X	Especifica que la versión actual del registro de KPI se mantendrá si se actualiza el registro. Editable cuando el valor @NX_ALWAYS_KEEP_KPI_VERSIONS en NX.env se establece en No.
Versión	X	X	X	Identifica el número de versión del registro de KPI. El número de versión aumenta automáticamente cada vez que se actualiza el registro. No editable.
Estado de registro	X	X	X	Especifica si el KPI está activo (recopilando datos) o inactivo (no recopilando datos). Editable solamente si se utiliza la función "Editar en Lista" en la página Lista de KPI.
Tipo de métrica	X	X	X	Especifica el tipo de cálculo que realizará el KPI. ■ Los KPI de consultas almacenadas son siempre del tipo Número. ■ Los KPI del sistema pueden ser del tipo Número o Duración. ■ Los KPI de SQL pueden ser del tipo Número, Suma, Máx, o Duración. Editable solamente para los KPI de tipo SQL.
Actualizar Hora	X	X	X	Especifica el intervalo de tiempo para recuperar las métricas de los KPI de la base de datos. El valor se puede editar. El tiempo de actualización se especifica en el formato HH:MM:SS.
Proceso Tipo	X			Las métricas de los KPI del sistema se pueden obtener de los siguientes procesos de CA Service Desk Manager: ■ domsrvr: gestor de objetos

Campo	Sys.	S.Q.	SQL	Descripción
				■ bpvirtddb: servidor de la base de datos virtual BOP ■ db_agents: agentes de base de datos ■ webengine: el servicio Web de CA Service Desk Manager Para obtener más información sobre estos procesos, consulte KPI de sistema (see page 749).
Sistema Nombre	X			El nombre interno del KPI de sistema. No editable.
Usuario Contexto		X	X	(Opcional) Especifica el ID de usuario de un contacto de CA Service Desk Manager. Las asignaciones de cliente y rol del contacto se utilizan para determinar las particiones de datos para las métricas generadas por el KPI. El valor se puede editar.
Almacenada Consulta		X		El nombre de la consulta almacenada llamada por este KPI. El valor se puede editar.
SQL Consulta			X	Código SQL de la consulta. El valor se puede editar.
Descripción	X	X	X	(Opcional) Ofrece una descripción detallada del propósito del KPI. El valor se puede editar.

Recuperación de datos del ticket

Para permitir la generación de informes sobre cuánto tiempo permanecen los tickets en los diferentes estados de procesamiento, puede configurar el daemon de KPI para recuperar datos sobre tickets de CA Service Desk Manager siempre que se abra o cierre un ticket y siempre que se modifique cualquiera de los valores siguientes:

- Activo
- Asignado
- Área o categoría
- Group
- Impacto
- Organization
- Prioridad
- Causa raíz

- Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.
- Tipo de servicio

Para activar la función de recuperación de tickets, instale la opción Tabla de datos de ticket de KPI disponible en la carpeta KPI del gestor de opciones.

La recopilación de datos de tickets nuevos y actualizados queda activada. Los datos de tickets se escriben en la tabla de base de datos `usp_kpi_ticket_data` y están disponibles para generar informes basados en Web.

Nota: Para obtener instrucciones, consulte la *Ayuda en línea*.

Las consideraciones siguientes se aplican a la recuperación de tickets:

- El daemon de KPI puede tardar hasta 30 minutos para rellenar la información del ticket en la tabla `usp_kpi_ticket_data`.
- El campo `support_lev` permite realizar un seguimiento del procesamiento de tipo de servicio cuando está instalada la opción `classic_sla_processing`. La opción `classic_sla_processing` habilita el procesamiento del tipo de servicio a partir de la versión 6.0 de CA Service Desk Manager y anteriores.
- La activación de esta función puede tener como resultado una reducción del rendimiento de CA Service Desk Manager.

Más información:

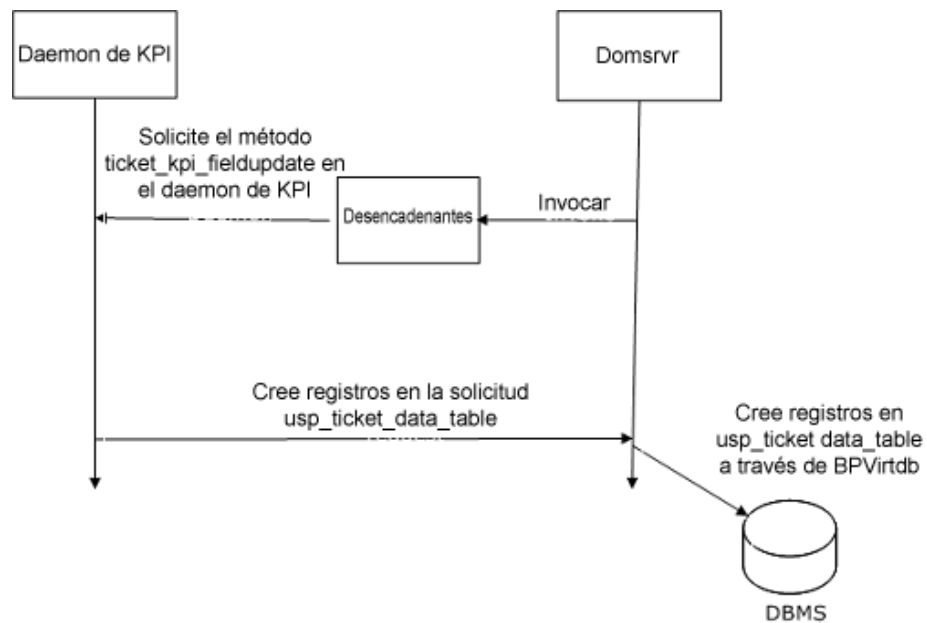
[Archivo NX.env](#) (en la página 758)

Flujo de datos del ticket de KPI:

La característica Tabla de datos de ticket de KPI funciona con un mecanismo de activación. Cuando se instala la opción `kpi_ticket_data_table`, el daemon de KPI comienza a controlar los objetos del ticket de CA Service Desk Manager para realizar el seguimiento de los siguientes eventos:

- Apertura de un nuevo ticket
- Comprobación de los cambios en uno o más campos controlados
- Cierre de un ticket

Cuando se produce uno de estos eventos, se activa un desencadenador `POST_CI`. El desencadenador envía un `BPMMessage` con una lista de atributos de desencadenador al daemon de KPI, y agrega los datos devueltos a la tabla `usp_kpi_ticket_data`, como se ilustra en el siguiente diagrama de flujo de datos.



Tipos de registros de Tabla de datos de ticket de KPI

Hay cinco tipos de operación en la tabla `usp_kpi_ticket_data`:

- `INIT (0)`
- `NO_INIT_REC (1)`
- `REOPEN (2)`
- `UPDATE (3)`
- `CLOSE (4)`

El valor de tipo (valor entero que se muestra entre paréntesis) se almacena en el campo de operación. El end_time del registro anterior se almacena en el campo prev_time. El campo ktd_duration almacena la duración, que se calcula como end_time menos prev_time. El registro anterior se define en las reglas siguientes:

1. El registro INIT indica que se ha creado un ticket.
2. Se crea un registro UPDATE por cada actualización para un ticket. Si existe un registro de UPDATE anterior, obtiene prev_time de éste para el mismo campo de ticket. En los demás casos, obtiene prev_time de los registros INIT, NO_INIT_REC o REOPEN, en función del registro que tenga el valor de end_time más próximo en el tiempo al registro UPDATE.
3. El registro CLOSE equivale a UPDATE.
4. Si un ticket se vuelve a abrir, se crea un solo registro REOPEN para mostrar el valor del campo Activo. El registro REOPEN obtiene prev_time de un registro CLOSE anterior para el mismo campo Activo.
5. Si un ticket se crea antes de activar la opción Gestor de opciones, quizás tiene registros para actualizaciones, sin contar con un registro INIT. En este caso, el programa crea un registro NO_INIT_REC y obtiene prev_time del primer registro que no sea INIT que encuentre.

Nota: Para obtener la documentación completa de los campos de la tabla, consulte la *Guía de referencia técnica*.

Solución de problemas

Se pueden diagnosticar los problemas que podrían suceder con el uso de KPI.

Compruebe que el daemon de KPI se esté ejecutando.

Para verificar que el daemon de KPI se está ejecutando, ejecute la utilidad de línea de comandos pdm_status de la siguiente manera:

```
pdm_status
```

Examine el resultado para encontrar lo siguiente:

```
KPI Daemon myserver Running myserver 3568 Wed Feb 06 07:23:53
```

Archivo NX.env

Revise el archivo \$NX_ROOT/NX.env para comprobar que se haya definido correctamente la configuración de KPI básica.

Si ha instalado la opción Tabla de datos de ticket de KPI, el archivo de NX.env incluye lo siguiente:

```
#####
# NX_KPI_TICKET_DATA_TABLE
# Enable the collection of changed fields from ticket objects
# (like Requests, Issues and Change Orders) to write record entries
# into the usp_kpi_ticket_data table.
#####
@NX_KPI_TICKET_DATA_TABLE=Yes

#####
# NX_KPI_FUZZ_TIME
# Specifies a tolerable delay for each KPI within which kpi_daemon
# sends a request to retrieve KPI data when this KPI's refresh time
# is timeout
#####
@NX_KPI_FUZZ_TIME=20
```

Nota: El valor predeterminado del parámetro @NX_KPI_FUZZ_TIME es 20 segundos. Se puede modificar este valor dentro del intervalo de 0 a 40 segundos. Si esta variable se establece en un valor mayor que 40, se utilizará 40 segundos.

```
#####
# NX_ALWAYS_KEEP_KPI_VERSIONS
# The keep_version attribute in kpi table is displayed on the KPI
# Detail Edit form as a checkbox. The NX_ALWAYS_KEEP_KPI_VERSIONS
# option specifies that checkbox is read-only and is always checked.
#####
@NX_ALWAYS_KEEP_KPI_VERSIONS=Yes
```

Activación del seguimiento del daemon de KPI

La utilidad pdm_logstat permite activar el registro de seguimiento para la supervisión de la actividad del daemon de KPI.

Para activar el seguimiento del daemon de KPI, ejecute el siguiente comando:

```
pdm_logstat -f cache_table_mgr.c VERBOSE
```

Para desactivar el seguimiento del daemon de KPI, ejecute el siguiente comando:

```
pdm_logstat -f cache_table_mgr.c
```

Examine el archivo stdlog.0 para buscar entradas que pertenezcan a la actividad del daemon de KPI.

El ejemplo siguiente muestra las conexiones normales del daemon de KPI al equipo host y domsrvr:

```
02/06 05:42:14.58 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT kpi_daemon.c 117 KPIDaemon ready for action!
02/06 05:42:14.80 garbo-2k3-bb domsrvr 792 SIGNIFICANT connmgr.c 2314 Connecting client kpi_daemon:garbo-2k3-bb
02/06 05:42:14.81 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT main.c 220 KPI daemon connected with domsrvr
```

El siguiente ejemplo indica un error en un KPI denominado webSessionCT:

```
01/16 13:24:46.74 jed web:local 2152 ERROR sys_kpi.c 96 Invalid KPI metric type: 1382180215 (KPI name:webSessionCT)
```

Los siguientes ejemplos muestran la actividad del daemon de KPI:

```
02/06 07:23:50.47 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache Table manager created kpi_obj (KPI dob record_id:9003) (KPI type:2)
02/06 07:23:50.53 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache Table manager created kpi_obj (KPI dob record_id:9103) (KPI type:1)
```

Nota: Para obtener más información sobre los tipos de KPI, consulte Tipos de registros de Tabla de datos de ticket de KPI (see page 756).

Escritura de informes de CA Business Intelligence

Puede escribir informes de CA Business Intelligence para CA Service Desk Manager.

Más información:

[Controlador ODBC de CA Service Desk Manager](#) (en la página 759)

[Escribir SQL para informes de BusinessObjects](#) (en la página 760)

[Funciones PDM](#) (en la página 761)

[Alias de atributo](#) (en la página 764)

[SQL interactivo de pdm isql](#) (en la página 764)

Controlador ODBC de CA Service Desk Manager

Las aplicaciones de informes BusinessObjects (informes de Crystal y Web Intelligence) acceden a los datos mediante un controlador ODBC que se conecta directamente con el motor de objetos de CA Service Desk Manager (domsrvr).

Esta conexión proporciona un número de beneficios:

- Declaraciones SELECT utilizadas por objetos de referencia de informes de BusinessObjects y atributos que utilizan sus nombres de CA Service Desk Manager (dicho de otra manera, sus nombres Majic). Por ejemplo, una declaración SELECT para un informe sobre contactos se podría escribir:
`SELECT combo_name FROM cnt WHERE last_name LIKE 'smith%'`
- El controlador ODBC de CA Service Desk Manager asigna atributos como combo_name y objetos como cnt al nombre o nombres de DBMS correspondientes.
- Toda la seguridad de CA Service Desk Manager, incluidas la partición de datos y las restricciones de cliente, se aplica automáticamente a los informes. Todas las conexiones entre BusinessObjects y CA Service Desk Manager se asocian con un contacto de CA Service Desk Manager, y el ODBC de CA Service Desk Manager edita declaraciones SELECT de entrada para exigir las restricciones de seguridad asociadas con el rol de informe de usuario de final. BusinessObjects no se conecta directamente a la base de datos.
- La opción Alias de atributo de CA Service Desk Manager se "aplana" o desnormaliza la base de datos de CA Service Desk Manager. Los alias de atributo son atributos adicionales en objetos de CA Service Desk Manager que admiten que una consulta haga referencia a atributos dentro tablas unidas sin una unión explícita, lo que permite que la tabla base se use como si fuera una vista de informe.
- El controlador ODBC de CA Service Desk Manager admite frases literales de fecha en consultas y traduce automáticamente los valores del formato de fecha interno de CA Service Desk Manager a una fecha de DBMS estándar.

Importante: El controlador ODBC de CA Service Desk Manager es compatible solamente con informes de BusinessObjects (Cristal y Web Intelligence). CA Service Desk Manager no proporciona un cliente de ODBC independiente y no recomienda el uso del controlador ODBC con otras aplicaciones que no sean BusinessObjects.

Escribir SQL para informes de BusinessObjects

Todas las declaraciones SQL utilizadas por informes de BusinessObjects son procesadas por el controlador ODBC de CA Service Desk Manager. El controlador ODBC es compatible con declaraciones SELECT SQL 92 con los siguientes cambios y extensiones:

- Los nombres de objetos de CA Service Desk Manager se utilizan en lugar de los nombres de tablas de DBMS, y los nombres de atributos de CA Service Desk Manager se utilizan en lugar de los nombres de columnas de DBMS.

- Un nombre de alias de atributo de CA Service Desk Manager se puede utilizar en cualquier parte de la consulta donde un nombre de columna sea válido. El controlador ODBC reemplaza la referencia del alias de atributo con una o más uniones.

Nota: Para obtener más información, consulte Alias de atributo (see page 764).

- Los atributos DERIVED de CA Service Desk Manager (como combo_name) sólo se pueden utilizar en la lista de selección. No son compatibles en ninguna otra parte de la consulta, incluso en la cláusula WHERE.

Nota: Se han proporcionado muchos nombres combinados con objetos de ID de usuario en el universo, como el nombre combinado de cliente con objeto de ID de usuario utilizado como filtro en el informe ad hoc de ejemplo que aparece en la *Guía de administración*. Estos objetos permiten que el nombre combinado se use como mensajes de filtro en consultas ad hoc con Web Intelligence, para superar la limitación de incluir el nombre combinado en la cláusula WHERE. Presentan nombre combinado e ID del usuario en el mensaje de filtro, pero utilizan sólo los ID de usuario seleccionados en la consulta de SQL resultante.

- Las consultas pueden contener frases literales de fecha con cualquiera de estos formatos:

d'aaaa-mm-dd hh:mm:ss xm' (donde xm es a.m. o p.m.)

ts'aaaa-mm-dd hh:mm:ss'

Estas frases literales se pueden utilizar en cualquier parte de la consulta. El controlador ODBC los convierte automáticamente en el formato de fecha interno de CA Service Desk Manager (el número de segundos desde la medianoche del 1 de enero de 1970).

Funciones PDM

Para brindar asistencia al trabajar con opciones y tipos de datos de CA Service Desk Manager especializados, el controlador ODBC extiende SQL para que sea compatible con un número de funciones de consulta adicionales. Todas las funciones compatibles con el controlador comienzan con la cadena "Pdm" y se conocen como funciones PDM según se describe en la siguiente tabla:

Funciones PDM	Descripción
PdmAddDays([date,] count)	Cuando se usa con un argumento, agrega el número de días en su argumento a la fecha actual y devuelve el resultado. Cuando se usa con dos argumentos, agrega el número de días en su segundo argumento al valor de la columna de fecha especificada en su primer argumento y devuelve el resultado. Esta función se puede utilizar en cualquier parte de la consulta
PdmAddMonths([date,]	Cuando se usa con un argumento, agrega el número de meses en su

Funciones PDM	Descripción
count)	argumento a la fecha actual y devuelve el resultado. Cuando se usa con dos argumentos, agrega el número de meses en su segundo argumento al valor de la columna de fecha especificada en su primer argumento y devuelve el resultado. El formulario de argumento único se puede utilizar en cualquier parte de la consulta. El formulario de dos argumentos se puede utilizar solamente en la lista de selección.
PdmDay([date])	Cuándo se usa sin argumentos, devuelve el día actual como entero. Cuándo se usa con un argumento, devuelve el día asociado con el valor de la columna de fecha especificada en su argumento. El formulario de argumento cero se puede utilizar en cualquier parte de la consulta. El formulario de un argumento se puede utilizar solamente en la lista de selección.
PdmDownTime(slaName, workshift, startDate, endDate)	Calcula el tiempo de reposo entre dos fechas en el SLA y el calendario especificados. Esta función se puede utilizar solamente en la lista de selección.
PdmMonth([date])	Cuando se utiliza sin argumentos, devuelve el mes actual como un entero de 1 a 12. Cuando se usa con un argumento, devuelve el mes asociado con el valor de la columna de fecha especificada en su argumento. El formulario de argumento cero se puede utilizar en cualquier parte de la consulta. El formulario de un argumento se puede utilizar solamente en la lista de selección.
PdmMonthName([date])	Cuando se utiliza sin argumentos, devuelve el nombre localizado del mes actual ("Enero", "Febrero" y así sucesivamente). Cuando se usa con un argumento, devuelve el nombre localizado del valor de la columna de fecha especificada en su argumento. El formulario de argumento cero se puede utilizar en cualquier parte de la consulta. El formulario de un argumento se puede utilizar solamente en la lista de selección.
PdmDay([date])	Cuándo se usa sin argumentos, devuelve el día actual como entero. Cuándo se usa con un argumento, devuelve el día asociado con el valor de la columna de fecha especificada en su argumento. El formulario de argumento cero se puede utilizar en cualquier parte de la consulta. El formulario de un argumento se puede utilizar solamente en la lista de selección.
PdmSeconds(date)	Devuelve el valor de la columna de fecha especificada en su argumento sin formato como el número de segundos desde la medianoche del 1 de enero de 1970. Esta función se puede utilizar solamente en la lista de selección. Tenga en cuenta que se requiere el argumento.
PdmString(column)	Devuelve la cadena equivalente del valor de la columna especificada en su argumento. Esta función se puede utilizar con columnas de UUID, fecha, o cadena. Se puede utilizar solamente en la lista de selección.
PdmToday()	PdmToday ([timeAdj [, day [, month [, year]]]]) Devuelve la fecha actual en segundos desde 1/1/1970. Esta función se

Funciones PDM	Descripción
	puede utilizar en cualquier parte de la consulta. Los siguientes argumentos ajustan la fecha devuelta: timeAdj ■ -1 => ajustan la hora al inicio del día (0:00:00; ■ +1 => ajustan la hora al final del día (23:59:59) día ■ negativo => ajustan la fecha según el número de días especificados ■ positivo => establecen el día en el valor absoluto especificado (o en el último día del mes; lo que sea menor) mes ■ negativo => ajustan la fecha según el número de meses especificados ■ positivo => establecen el mes en el valor absoluto especificado (o en Diciembre (12); lo que sea menor) año ■ negativo => ajustan la fecha según el número de años especificados ■ positivo => establecen el año en el valor absoluto especificado Los ajustes se aplican en el orden año, mes, día. Se pasan por alto el cero o los argumentos omitidos.
PdmYear([date])	Cuando se usa sin argumentos, devuelve el año actual como un entero de cuatro dígitos. Cuando se usa con un argumento, devuelve el año asociado con el valor de la columna de fecha especificada en su argumento. El formulario de argumento cero se puede utilizar en cualquier parte de la consulta. El formulario de un argumento se puede utilizar solamente en la lista de selección.

Alias de atributo

Los alias de atributo son atributos adicionales en objetos de CA Service Desk Manager que hacen referencia a datos de tablas unidas usando sintaxis de unión separada por puntos Majic (donde la sintaxis `srelname.attrname` es una referencia al atributo `attrname` en la tabla a la cual hace referencia la clave externa `srelname`). Se proporciona un gran número de alias de atributo predefinidos con CA Service Desk Manager r12.5, con nombres que son normalmente iguales que la correspondiente unión Majic, con guiones bajos que sustituyen los puntos que indican la unión. Por ejemplo, la siguiente declaración SELECT se puede utilizar para un informe que contiene información sobre los asignatarios de la solicitud:

```
SELECT ref_num, assignee_combo_name, assignee_organization_name
FROM cr WHERE customer_last_name LIKE 'smith%'
```

El controlador ODBC de CA Service Desk Manager crea uniones automáticamente según se requiera para acceder las tablas a las que hacen referencia los alias de atributo. Un usuario con el rol de administrador de CA Service Desk Manager puede agregar fácilmente nuevos alias de atributo en línea, proporcionando una forma de una columna a la vez para extender la vista correspondiente a un objeto.

Para acceder a la tabla Alias de atributo, seleccione la ficha Administración y vaya a CA Service Desk Manager, Códigos, Alias de atributo.

SQL interactivo de pdm_isql

Con CA Service Desk Manager se proporciona una utilidad de línea de comandos, `pdm_isql`, para permitir la entrada interactiva de declaraciones SQL SELECT. Las declaraciones SELECT introducidas en `pdm_isql` se envían al controlador ODBC de CA Service Desk Manager, lo que le permite probar declaraciones SQL SELECT fuera de BusinessObjects.

Para utilizar pdm_isql

1. Asegúrese de que `$NX_ROOT/bin` esté en la ruta.
2. Escriba el siguiente comando:
`pdm_isql`

3. En el símbolo del sistema `pdm_isql`, escriba el siguiente comando:

```
connect username*password@casd_hostname
```

(Donde *username* y *password* son credenciales de inicio de sesión de CA Service Desk Manager válidos y el nombre de host es el nombre de host de un servidor de CA Service Desk Manager con un motor Web.)

4. Introduzca declaraciones SQL `select` seguidas por un punto y coma.

Capítulo 18: Generación de informes en CA Service Desk Manager

Esta sección contiene los siguientes temas:

[Generación de informes](#) (en la página 767)
[Vistas de las bases de datos](#) (en la página 767)
[Configuración de métodos de generación de informes](#) (en la página 771)
[Formato de informes](#) (en la página 771)
[Modificación del orden de clasificación de columnas](#) (en la página 772)
[Informes de resumen y detalles](#) (en la página 772)
[Informes de análisis](#) (en la página 773)

Generación de informes

CA Service Desk Manager ofrece diversas capacidades y opciones integradas de generación de informes que permiten:

- imprimir formularios para activos y órdenes de cambio, incidencias, incidentes, problemas individuales, etc.
- Genere informes resumidos o detallados relativos a listas de órdenes de cambio, incidencias, solicitudes, problemas, elementos de configuración, etc.
- Genere informes de análisis.

Nota: Para obtener más información sobre cómo utilizar los informes de CA Service Desk Manager, consulte Generación de informes en la *Ayuda en línea*. Además de emplear las funciones de generación de informes incorporadas en CA Service Desk Manager, es posible crear y generar informes personalizados basados en las tablas y las vistas de la base de datos de CA Service Desk Manager. Para obtener más información sobre informes personalizados, consulte la *Guía de implementación*.

Vistas de las bases de datos

Las bases de datos de CA Service Desk Manager son repositorios donde se guardan los datos indicados y usados para hacer funcionar el servicio de asistencia. CA Service Desk Manager dispone de varias vistas y permite la creación de informes personalizados relativos a las bases de datos.

Las vistas son de dos clases:

- Básica
- Avanzada

Más información:

[Descripciones de los campos de vista](#) (en la página 947)

Vistas básicas

Las vistas básicas se basan en las tablas de CA Service Desk Manager. Estas vistas muestran datos mientras la implementación haga uso de las solicitudes, los incidentes, los problemas, las órdenes de cambio, las incidencias, los activos, o bien, los contactos o grupos.

El uso de las vistas básicas permite diseñar y producir numerosos informes como los siguientes:

- Listas detalladas y resumidas de solicitudes de prioridad 1 abiertas, ordenadas por área de solicitud.
- Listas detalladas y resumidas de órdenes de cambio asignadas al grupo de nivel 1 que lleven abiertas más de 24 horas, ordenadas por prioridad.
- Recuentos de incidencias que lleven abiertas más tiempo que el número especificado de días, ordenadas por prioridad, por el grupo asignado o por la prioridad y el grupo asignado

Se proporcionan las vistas básicas siguientes:

Nombre de la vista	Descripción
View_Contact_Full	Todos los contactos, con inclusión del tipo de contacto, la ubicación, las organizaciones y los tipos de servicios
View_Contact_to_Environment	Todos los contactos y su entorno (activos)
View_Group	Todos los grupos definidos en la base de datos
View_Group_To_Contact	Todos los contactos (incluidos gestores) dentro de sus asignaciones de grupo
View_Request	Todas las solicitudes, con inclusión de sus tipos de servicios, la gravedad, la urgencia, las categorías, los activos, los números de impacto, los asignatarios por nombre, los clientes por nombre, los grupos, los estados y las prioridades
View_Act_Log	Información de los registros de actividades de las solicitudes, con inclusión del tipo de actividad y del

Nombre de la vista	Descripción
	nombre del analista
View_Request_to_Act_Log	Todas las solicitudes con sus registros de actividades (aúna las vistas View_Request y View_Act_Log)
View_Request_to_Properties	Solicitudes y sus propiedades (puede no incluir todas las solicitudes, en especial si no tienen asignada ninguna propiedad)
View_Change	Todas las órdenes de cambios, con inclusión de sus estados, las prioridades, las categorías, las organizaciones, los usuarios finales afectados por nombre, los solicitantes por nombre, los asignatarios por nombre, los grupos, los tipos de servicios y los números de impacto
View_Change_Act_Log	Información de los registros de actividades de las órdenes de cambios
View_Change_to_Change_Act_Log	Todas las órdenes de cambios con sus registros de actividades (aúna las vistas View_Change y View_Change_Act_Log)
View_Change_to_Properties	Órdenes de cambios y sus propiedades (puede no incluir todas las órdenes de cambios, en especial si no tienen asignada ninguna propiedad)
View_Change_to_Change_WF	Órdenes de cambios y sus tareas de workflow (puede no incluir todas las órdenes de cambios, en especial si no tienen asignada ninguna tarea de workflow)
View_Change_to_Assets	Órdenes de cambios y sus activos (puede no incluir todas las órdenes de cambios, en especial si no tienen ningún activo)
View_Change_to_Requests	Órdenes de cambios con información básica sobre las solicitudes adjuntas (aúna las vistas View_Change y Call_Request; puede no incluir todas las órdenes de cambios, en especial si no se les ha adjuntado ninguna solicitud)
View_Issue	Todas las incidencias, con inclusión de sus estados, las prioridades, las categorías, las organizaciones, los usuarios finales afectados por nombre, los asignatarios por nombre, los grupos, los tipos de servicios, etc.
View_Issue_Act_Log	Información de los registros de actividades de las incidencias
View_Issue_to_Issue_Act_Log	Todas las incidencias con sus registros de actividades (aúna las vistas View_Issue y View_Issue_Act_Log)
View_Issue_to_Properties	Incidencias y sus propiedades (puede no incluir todas

Nombre de la vista	Descripción
	las incidencias, en especial si no tienen asignada ninguna propiedad)
View_Issue_to_Issue_WF	Incidencias y sus tareas de workflow (puede no incluir todas las incidencias, en especial si no tienen asignada ningún workflow)
View_Issue_to_Assets	Incidencias y sus activos (puede no incluir todas las incidencias, en especial si no tienen ningún activo)

Vistas avanzadas

Las vistas avanzadas se basan en la tabla audit_log de CA Service Desk Manager.

Nota: Es preciso instalar las opciones audit_ins o audit_upd en el gestor de opciones y reiniciar el sistema para poder utilizar estas vistas.

El uso de las vistas avanzadas permite generar informes sobre la duración de los partes (esto es, solicitudes, órdenes de cambios o incidencias) en un estado en particular. Por ejemplo, se puede informar de lo siguiente:

- Mostrar el tiempo transcurrido entre la apertura y la asignación al nivel 2 de las solicitudes abiertas desde el 1 de enero de 2002
- Mostrar el tiempo en que las incidencias abiertas desde el 1 de enero de 2002 han permanecido en la prioridad 3 antes de pasar a la prioridad 2.

Se proporcionan las siguientes vistas avanzadas, que son vistas de la tabla audit_log de la base de datos de CA Service Desk Manager que realizan consultas específicas sobre los atributos de estado, prioridad, grupo o asignatario:

Nombre de la vista	Descripción
View_Audit_Status	Todos los tickets clasificados por el tiempo transcurrido en cada estado (no incluye los tickets que carecen de estado)
View_Audit_Priority	Todos los tickets clasificados por el tiempo transcurrido en cada prioridad
View_Audit_Group	Todos los tickets clasificados por el tiempo transcurrido en cada asignación de grupo (no incluye los tickets que carecen de grupo)
View_Audit_Assignee	Todos los tickets clasificados por el tiempo transcurrido en cada asignación individual (no incluye los tickets que carecen de asignatario)

Importante: es preciso instalar las opciones de registro de auditoría con el gestor de opciones para ver los datos de las vistas avanzadas. Si desea obtener más información, consulte las descripciones de las opciones de auditoría audit_ins y audit_upd de la Ayuda en línea.

Más información:

[Uso del Gestor de opciones](#) (en la página 355)

Configuración de métodos de generación de informes

Los métodos de generación de informes permiten especificar adónde se deben enviar los resultados de los informes al seleccionar éstos. Entre otros ejemplos, se podrían citar los informes resumidos y detallados que están disponibles en el menú Informes y los informes disponibles en el menú Análisis. Se ofrecen varios métodos predefinidos que se pueden modificar.

Nota: Para obtener más información sobre la definición de métodos de generación de informes, consulte la *Ayuda en línea*.

Formato de informes

Con el archivo dataent.fmt, ubicado en el directorio \$NX_ROOT/fig/cfg (UNIX) o directorio_instalación\fig\cfg (Windows), es posible personalizar los diversos formatos de datos en los informes que se impriman. este archivo se visualiza y modifica con cualquier editor de texto (en Windows, se utiliza WordPad para editarlo).

Las líneas siguientes del archivo sirven para controlar algunos de los formatos de la fecha y la hora:

```
default_date = "long_date"
short_date = "M/D/YY// Escriba una fecha con el formato MM/DD/YY"
long_date = "MM/DD/YYYY// Escriba una fecha con el formato MM/DD/YY"
default_tod = "hour_12"
hour_12 = "h:mm:ss a(am,pm)// Escriba una hora con el formato hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Escriba una hora con el formato 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Escriba una hora con el formato hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Escriba una hora con el formato 00:00:00 - 23:59:59"
default_date_time = "date_time12"
date_time12 = "D/MM/YYYY h:mm:ss a(am,pm)// Escriba una fecha y una hora con el formato DD/MM/YY hh:mm:ss am/pm"
date_time24 = "D/MM/YYYY HH:mm:ss// Escriba una fecha y una hora con el formato DD/MM/YY 00:00:00-23:59:59"
```

A continuación, se ejemplifica cómo modificar estas líneas de manera que se adapten a los formatos de fechas y horas que se suelen emplear en los países europeos:

```
default_date = "long_date"
short_date = "D/M/YY// Escriba una fecha con el formato DD/MM/YY"
long_date = "DD/MM/YYYY// Escriba una fecha con el formato DD/MM/YYYY"
default_tod = "hour_24"
hour_12 = "h:mm:ss a(am,pm)// Escriba una hora con el formato hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Escriba una hora con el formato 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Escriba una hora con el formato hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Escriba una hora con el formato 00:00:00 - 23:59:59"
default_date_time = "date_time24"
date_time12 = "D/MM/YYYY h:mm:ss a(am,pm)// Escriba una fecha y una hora con el formato DD/MM/YY hh:mm:ss am/pm"
date_time24 = "D/MM/YYYY HH:mm:ss// Escriba una fecha y una hora con el formato DD/MM/YY 00:00:00-23:59:59"
```

Nota: Si emplea pdm_extract para exportar datos de las bases de datos de CA Service Desk Manager a otros sistemas y desea extraer los datos de forma que sigan el formato especificado en el archivo dataent.fmt, use el modificador -d al invocar pdm_extract.

Modificación del orden de clasificación de columnas

Los administradores pueden modificar el orden de clasificación de las columnas que aparecen en los informes utilizando Web Screen Painter.

Los usuarios pueden clasificar los datos en los siguientes órdenes:

- ascendente (de la A a la Z, de cero a 9 o de la fecha más antigua a la más reciente)
- descendente (de la Z a la A, del 9 al cero o de la fecha más reciente a la más antigua)

Nota: Para obtener más información, consulte la *Ayuda de Web Screen Painter*.

Informes de resumen y detalles

CA Service Desk Manager incorpora opciones para la generación de informes resumidos y detallados. Para hacerlo, se puede usar la función de búsqueda de las ventanas de lista. Así, por ejemplo, es posible indicar criterios de búsqueda en la ventana Lista de solicitudes para crear una lista de solicitudes aptas para la generación del informe.

Para imprimir o ver los informes resumidos y detallados, antes es necesario seleccionar los registros que se deseen incluir en el informe en cuestión. Además, si se desea imprimir un informe detallado de una sola página por cada registro, se puede hacer seleccionando la opción Imprimir formulario del menú Archivo de cualquier página de detalles. Para imprimir informes relativos a registros recién creados, primero es necesario guardar éstos.

Nota: Para obtener más información sobre el uso de informes, consulte la *Ayuda en línea*.

Informes de análisis

La ficha Administración de CA Service Desk Manager también ofrece los siguientes informes de análisis incorporados, con los que es posible obtener una perspectiva global y detallada de los procesos del servicio de asistencia:

- Informes de solicitudes o incidencias
- Informes de áreas de solicitud o categorías de incidencias
- Informes de prioridad de áreas de solicitud o prioridad de categorías de incidencias

Se pueden mostrar los informes de análisis del día actual, de los últimos treinta días o de lo que va de año hasta la fecha.

Más información:

[Generación de informes de solicitudes o incidencias](#) (en la página 773)

[Generación de informes de áreas de solicitud o categorías de incidencias](#) (en la página 774)

[Generación de informes de prioridad de áreas de solicitud o prioridad de categorías de incidencias](#) (en la página 774)

Generación de informes de solicitudes o incidencias

Los informes de solicitudes o incidencias proporcionan estadísticas de períodos concretos relativas, por ejemplo, al número de solicitudes o incidencias que se han abierto o cerrado, al tiempo medio de apertura o al tiempo medio transcurrido hasta su cierre. Estos informes se ordenan por fecha, de la más antigua a la más reciente.

Para generar un informe de solicitudes o incidencias con la interfaz Web:

1. Seleccione la ficha Administración.
2. Expanda los nodos Service Desk y Análisis.

3. Seleccione Solicitud o Incidencia.
4. Seleccione el informe oportuno según el marco temporal que le interese.

Generación de informes de áreas de solicitud o categorías de incidencias

Los informes de áreas de solicitud o categorías de incidencias indican el número de solicitudes o incidencias que se han abierto durante el período especificado por cada área de solicitud o categoría de incidencias. Este informe se ordena alfabéticamente por área de solicitud o categoría de incidencias.

Para generar un informe de áreas de solicitud o categorías de incidencias con la interfaz Web:

1. Seleccione la ficha Administración.
2. Expanda los nodos Service Desk y Análisis.
3. Seleccione Solicitud o Incidencia.
4. Seleccione el informe oportuno según el marco temporal que le interese.

Generación de informes de prioridad de áreas de solicitud o prioridad de categorías de incidencias

Los informes de prioridad de áreas de solicitud o prioridad de categorías de incidencias indican el número de solicitudes o incidencias que se han abierto por prioridad durante el período especificado por cada área de solicitud o categoría de incidencias. Este informe se ordena por prioridad (de mayor a menor) y, luego, alfabéticamente por área de solicitud o categoría de incidencias.

Para generar un informe de prioridad de áreas de solicitud o prioridad de categorías de incidencias con la interfaz Web:

1. Seleccione la ficha Administración.
2. Expanda los nodos Service Desk y Análisis.
3. Seleccione Solicitud o Incidencia.
4. Seleccione el informe oportuno según el marco temporal que le interese.

Capítulo 19: Gestión de conocimiento

Esta sección contiene los siguientes temas:

[Gestión del conocimiento](#) (en la página 775)

[Búsqueda de procedimientos para la gestión de conocimiento](#) (en la página 776)

[Conocimiento y multicitante](#) (en la página 776)

[Cómo configurar una base de conocimiento](#) (en la página 777)

[Cómo utilizar documentos en la base de conocimiento](#) (en la página 780)

[Archivos de conocimiento](#) (en la página 786)

[Búsqueda de conocimientos](#) (en la página 787)

[Foros](#) (en la página 788)

[Documentos de árbol de conocimientos](#) (en la página 788)

[Programación de documentos de conocimiento](#) (en la página 789)

[Acceso a exportación/importación](#) (en la página 799)

[Servicios Web](#) (en la página 814)

Gestión del conocimiento

La gestión del conocimiento se refiere al concepto de buscar, organizar y publicar el conocimiento. La gestión del conocimiento captura la información de manera rápida y eficaz y la entrega a un usuario o grupo. La información que se captura y se pone a disposición para su recuperación se conoce como base de conocimiento.

Los usuarios obtienen acceso a una base de conocimiento mediante un motor de búsqueda. Gestión del conocimiento le permite crear y gestionar el contenido que reside en una base de conocimiento. Es posible establecer permisos de categorías y de documentos que se utilizan en grupos o roles. Gestión del conocimiento colabora para ofrecer a los clientes soluciones para las incidencias complejas. La gestión del conocimiento eficaz se caracteriza por ofrecer rápidamente las soluciones para los clientes, a través de un proceso fácil de usar y recorrer.

Para gestionar eficazmente el conocimiento, puede hacer lo siguiente:

- Crear una jerarquía de contenido significativa.
- Identificar los vacíos en el conocimiento existente.
- Realizar actualizaciones y mantenimiento para garantizar la relevancia del contenido.
- Medir el valor del contenido disponible.

Más información:

[Configuración de restricciones para la partición de datos de Gestión del conocimiento para permisos basados en roles](#) (en la página 193)

Búsqueda de procedimientos para la gestión de conocimiento

CA Service Desk Manager proporciona procedimientos detallados para la gestión de conocimiento en esta guía y en la *Ayuda en línea*.

Para encontrar procedimientos detallados para la gestión de conocimiento en la *Ayuda en línea*

1. Inicie sesión en CA Service Desk Manager.

Aparecerá la página principal de CA Service Desk Manager.

2. Realice alguna de las siguientes acciones:

- Haga clic en Ayuda, Ayuda en el menú principal y vaya a la *Ayuda en línea* en Administración, Gestión de conocimiento.

Aparecen los temas de Gestión de Conocimiento y puede desplazarse por la jerarquía para encontrar la información que desee.

- Haga clic en Ayuda, Ayuda acerca de esta ventana en el menú principal.

Aparece la *ayuda en línea* y muestra un tema de ayuda para la página acerca de la cual desea información.

Conocimiento y multicitente

Los documentos de conocimiento y las categorías del conocimiento pueden ser específicos del cliente, estar compartidos entre varios clientes o compartirse como públicos. Cuando busca un documento de conocimiento, los resultados se limitan a los documentos que pueden ver los clientes asociados con el ticket. Los resultados de la búsqueda de preguntas frecuentes son específicos del cliente. Las clasificaciones de los documentos de cliente públicos se deben mantener por separado para cada cliente.

A nivel del cliente se pueden administrar las siguientes definiciones:

- Contenido de acción
- Plantillas de documento
- Proceso de aprobación de conocimiento
- Documentos recomendados
- ROI de Gestión del conocimiento
- Informes

Todos los demás valores del sistema de Gestión del conocimiento se administran globalmente, a nivel del proveedor de servicios.

Nota: El multicliente se configura en el gestor de opciones mediante la ficha Administración.

Cómo configurar una base de conocimiento

La gestión del conocimiento eficaz supone mucho más que el desarrollo de una gran base de conocimiento. La gestión del conocimiento también implica la implementación de procesos y procedimientos para mantener un contenido relevante y preciso.

Para configurar una base de conocimiento, haga lo siguiente:

1. Analice cómo se utilizará la base de conocimiento y su alcance.
2. Considere quiénes son los clientes y cuál será la información que probablemente necesitarán.
3. Desarrolle un plan estratégico que identifique los problemas potenciales que pueden derivar en la necesidad de atención al cliente. Los problemas identificados le pueden guiar para determinar el contenido que debe residir en la base de conocimiento.
4. Ejecute el desarrollo de la base de conocimiento. Cree, organice, mantenga y proteja estos datos. Todas estas funciones se pueden llevar a cabo mediante Gestión del conocimiento.

Importación de datos de conocimiento de muestra

Para su uso y conveniencia, se proporcionan datos de conocimiento de muestra extraídos de Knowledge Broker, PCHowTo y Right Answers.

Para utilizar los datos de conocimiento de ejemplo, importe los datos a la base de datos de Gestión del conocimiento.

Nota: Para obtener más información sobre los datos de ejemplo de KT, consulte la *Guía de implementación*.

Control de la base de conocimiento

La eficacia de la base de conocimiento se puede controlar con las siguientes herramientas de generación de informes. Estas herramientas permiten ver estadísticas sobre la utilidad de los documentos y su eficacia para resolver problemas.

Tarjeta de informes de conocimientos

Muestra las estadísticas de los documentos creados. Cada usuario tiene su propia tarjeta de informes de conocimiento.

Informes basados en Web

Muestra la métrica que describe la manera en que el conocimiento satisface las necesidades del usuario. Algunas de las opciones que se utilizan con más frecuencia incluyen:

- Listado de los documentos a los que se accede con mayor frecuencia.
- Visualización de búsquedas de usuarios que no han devuelto resultados.

Reindización de la base de conocimiento

Los siguientes cambios de los valores de búsqueda requieren reindexar la base de conocimiento mediante la utilidad de reindexación de conocimientos:

- Después de importar el conocimiento
- Después de cambiar los valores de análisis
- Después de las supresiones en masa
- Cuando se producen fallos en las búsquedas

La reindexación es necesaria porque los documentos existentes no reflejan los cambios realizados en los sinónimos, las palabras irrelevantes, los términos especiales y otros parámetros de investigación hasta que no se hayan reindexado. Todos los sinónimos, palabras irrelevantes y términos especiales nuevos se deben reindexar para garantizar que las búsquedas por palabras clave de la base de conocimiento estén actualizadas y sean exactas.

La reindexación de conocimiento se puede ejecutar desde una línea de comandos. `pdm_k_reindex.exe` es el archivo ejecutable para la reindexación de conocimiento.

Nota: La reindexación de los documentos de la base de conocimiento puede ser lenta, dependiendo del tamaño de la base de datos. Se recomienda ejecutar la utilidad de reindexación de conocimiento después de haber realizado todos los cambios que procedan.

Reindexación y desindexación de la configuración de colas para procesamiento instantáneo y por lotes

Tanto la reindexación como la desindexación ejecutan un proceso por lotes, para incluir en una ejecución una cantidad de documentos predefinida. Estos procesos por lotes se utilizan para optimizar el rendimiento. El rendimiento del sistema aumenta cuanto más documentos se incluyan en el lote.

El número de documentos que se puede procesar es limitado; el límite depende del tamaño de los documentos y de los archivos adjuntos vinculados. El tamaño del documento se calcula en función del texto puro y sus adjuntos. No se consideran los elementos de imagen y formato.

Nota: Puede limitar el tamaño de los adjuntos; para ello, vaya a Biblioteca de adjuntos, Repositorios en la ficha Administración y edite el repositorio para establecer el tamaño límite del archivo (KB).

El tamaño máximo de lote recomendado se encuentra entre 2 y 12 MB (de acuerdo con el parámetro EBR_MAX_INDEX_BATCH_SIZE del archivo NX.env y el tamaño medio del documento).

- Si el tamaño medio del documento (incluidos los adjuntos) es de 0,1 MB aproximadamente, conserve la definición predeterminada en NX.env:

```
@EBR_MAX_INDEX_BATCH_SIZE=128
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=1
@NX_EBR_INDEX_QUEUE_ONLINE=Yes
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
```

Esta definición significa que un lote procesa 128 documentos, que las ejecuciones de los lotes se realizan cada intervalos de diez segundos y que cuando se ejecuta una reindexación, el intervalo de espera entre dos lotes es de un segundo.

- Si el tamaño medio del documento (incluidos los adjuntos) es de 0,5 MB aproximadamente, conserve la definición predeterminada en NX.env:

```
@EBR_MAX_INDEX_BATCH_SIZE=25
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=10
@NX_EBR_INDEX_QUEUE_ONLINE=No
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
```

Esta definición significa que un lote procesa 25 documentos, que las ejecuciones de los lotes se realizan cada intervalos de diez segundos y que cuando se ejecuta una reindexación, el intervalo de espera entre dos lotes es de diez segundos.

Cómo utilizar documentos en la base de conocimiento

Los documentos de conocimiento proporcionan información sobre el conocimiento que se almacena en la base de conocimiento. La creación de conocimiento de calidad requiere de la participación de varios individuos. Cada individuo es responsable de ejecutar tareas específicas a lo largo de las diferentes etapas del ciclo de vida de un documento de conocimiento. Los documentos de conocimiento residen en la base de conocimiento y se gestionan como parte del siguiente proceso continuo:

1. Identificación del contenido que se debe incluir en la base de conocimiento.

2. Creación de un documento de conocimiento.

Los documentos de conocimiento se colocan en las categorías que algunas organizaciones asignan a propietarios.

Nota: Cuando se crea o actualiza un documento, se coloca en la bandeja de entrada de un propietario. Hasta que se publican, los elementos de la Bandeja de entrada no aparecen como resoluciones ni se agregan a la base de conocimiento.

3. Revisión del documento.

Después de que un documento llega a una carpeta de la bandeja de entrada del panel de resultados, los usuarios pueden realizar las tareas asignadas al modificar los documentos de acuerdo con los roles que se les ha asignado.

Todos los usuarios que dispongan de permisos completos (lectura y escritura) en un determinado documento, podrán modificarlo. El propietario actual dispone de permisos completos en el documento, aunque no necesariamente se explicita el permiso de escritura. Los usuarios pueden crear versiones o retroceder a una versión anterior cuando surgen problemas con el documento.

4. Envío del documento.

Además del envío desde la interfaz de autoservicio de cliente o de empleado, el conocimiento también se puede enviar desde CA Service Desk Manager. Esta opción permite al analista enviar una nueva resolución desde un ticket existente. Esta opción también ofrece un vínculo entre un problema y su resolución, y puede ayudar a otros usuarios con problemas similares a encontrar una resolución.

5. Publicación del documento.

Se puede publicar el documento después de que haya pasado a través del ciclo del proceso de aprobación completo. Un documento publicado pasa a formar parte de la base de conocimiento visible en la fecha de inicio, que es la fecha actual de forma predeterminada. Sólo los grupos a los que se les han otorgado derechos de acceso pueden ver el documento. Un usuario con todos los permisos puede editar un documento publicado.

6. Evalúe y decida si se deben ejecutar las siguientes tareas:

- **Anular la publicación del documento:** El propietario del documento, un gestor de conocimientos o un administrador no permiten la publicación del documento para su edición.
- **Crear una versión de reproceso:** los usuarios con todos los permisos de edición pueden crear una versión borrador de reproceso de un documento publicado mientras el documento está en línea y disponible para verlo o realizar búsquedas. Una versión de reproceso comienza como una copia del documento que se sustituye en la base de conocimiento después de verificarlo y volverlo a publicar.

- **Retirar el documento:** El propietario del documento, un gestor de conocimientos o un administrador del sistema pueden retirar el documento de la base de conocimiento.

Se pueden definir las tareas que se ejecutan y quién ejecuta cada una para satisfacer la estructura del proceso de aprobación que existe en una organización.

Nota: Puede realizar el seguimiento de las actividades de conocimiento desde la ficha Registro de eventos en las páginas de detalles de contacto. Por ejemplo, si un usuario final visualiza un documento de conocimiento, el registro de eventos se actualiza para mostrar la acción realizada y un vínculo al documento. El registro de eventos también realiza el seguimiento del tiempo que el usuario tuvo abierto el documento.

Envío de conocimiento desde CA Service Desk Manager

Si adquiere un conocimiento que piensa que se debe agregar a la base de conocimiento, lo puede enviar para su consideración. Además de enviar conocimiento desde la interfaz de autoservicio, se lo puede enviar desde CA Service Desk Manager. Un analista puede enviar una nueva resolución a partir de un ticket existente, que proporciona un vínculo entre un problema y su resolución. Además, puede ayudar otros usuarios que tienen problemas similares a encontrar una resolución. En una organización que puede tener cientos de tickets abiertos en forma simultánea, esta posibilidad puede ahorrar un tiempo valioso.

Todos los documentos de conocimiento se deben asignar a una categoría de conocimiento. Si el área de incidente/solicitud en CA Service Desk Manager coincide con las categorías del conocimiento en Gestión del conocimiento, se selecciona automáticamente la categoría para el envío de conocimiento.

Envío de conocimiento desde el autoservicio

De forma predeterminada, cualquier usuario que ha iniciado sesión en Gestión del conocimiento puede enviar el conocimiento para su consideración en la página Enviar conocimiento. Esta página permite a un cliente enviar el conocimiento sin ponerse en contacto con el representante del centro de servicio al usuario local. Después de enviar el conocimiento, éste atraviesa un proceso de publicación en el que se revisa y edita antes de agregarlo a la base de conocimiento.

Es importante introducir la información en todos los campos que aparecen en la página Enviar conocimiento. Preste especial atención al completar el campo Resumen. Típicamente, este campo contiene una descripción general concisa del documento que se envía.

Atributos de Documento

Establecer los atributos de documento ayuda a gestionar los documentos en la agrupación de conocimiento. Los atributos de documento se pueden actualizar para asignar al documento un experto en la materia o propietario nuevos. También se puede especificar la fecha en que el documento estará disponible en la base de conocimiento y la fecha en que caduca. Al seleccionar plantillas de documento diferentes, puede modificar el aspecto de cada documento.

Permisos del documento

Puede establecer, ver y editar los permisos para un documento. Estos permisos se pueden asignar a diferentes grupos de individuos. Al establecer permisos, se puede decidir heredar permisos de la categoría principal de un documento o especificar nuevos permisos. De forma predeterminada, los documentos heredan los permisos de su categoría principal. Este valor predeterminado controla los permisos de acceso a nivel de la categoría en vez de hacerlo a nivel del documento.

Importante: al crear un documento de conocimiento, verifique que los permisos del documento incluyan los usuarios que más tarde pueden estar asignados en el documento mediante el proceso de aprobación. Cuando se asigna un grupo a un documento, los usuarios de ese grupo pueden no disponer de permiso para ver el documento. Si el documento está asignado a un usuario específico, las restricciones de partición de datos predeterminadas permiten al usuario ver el documento.

Edición de resoluciones

Con Gestión del conocimiento, puede crear documentos de conocimiento utilizando el editor HTML. Esta característica le permite modificar el campo Resolución de un documento de conocimiento con el formato *lo que se muestra es lo que se obtiene* (WYSIWYG). El uso del editor HTML mejora el proceso de creación al permitir crear documentos sin necesidad de escribir código HTML, aplicar formato al texto, insertar gráficos y tablas y crear vínculos a otros documentos. Estas acciones aceleran el proceso de escritura y también ofrecen un método sencillo para editar un documento para propósitos organizativos.

El editor de plantillas le permite hacer lo siguiente:

- **Ver código HTML:** Las fichas modo Diseño y modo Fuente de la barra de herramientas del editor HTML le permiten cambiar entre las distintas vistas.
- **Aplicar formato al texto:** Puede introducir el texto del documento directamente en la ventana Editor de HTML. Puede aplicar formato al texto mediante las opciones de la barra de herramientas y el menú.
- **Insertar gráficos:** Puede insertar un gráfico en el texto HTML seleccionando una imagen de la biblioteca de imágenes o cargando sus propios gráficos.
- **Insertar tablas:** En un documento de conocimiento, puede mostrar con claridad grandes cantidades de información a los usuarios. Puede utilizar tablas para aplicar formato a esta información en filas y columnas.
- **Insertar hipervínculos en otros documentos:** Puede insertar hipervínculos a documentos de conocimiento al crear o cambiar un documento de conocimiento. De esta manera, un documento de conocimiento puede estar vinculado a otros documentos o URL relevantes. Cuando se utiliza el editor HTML en modo Diseño, los hipervínculos aparecen como texto subrayado, en color azul.
- **Insertar contenido de acción:** Puede insertar contenido de acción (una URL dinámica) en el campo Resolución de un documento de conocimiento que, cuando sea seleccionado por el usuario final, cree un incidente, o ejecute alguna otra acción.

Preparación de la publicación del documento

Después de que se envía un documento de conocimiento, se lo prepara para la publicación estableciendo sus atributos y permisos. La asignación de controles tales como configuraciones y categorías son importantes para organizar los documentos de una manera eficaz.

Más información:

[Cómo utilizar documentos en la base de conocimiento](#) (en la página 780)

[Atributos de Documento](#) (en la página 783)

[Permisos del documento](#) (en la página 783)

Publicación del documento

Se puede publicar el documento después de que haya pasado a través del ciclo del proceso de aprobación completo. Un documento publicado pasa a formar parte de la base de conocimiento visible en la fecha de inicio, que es la fecha actual de forma predeterminada. Sólo los grupos a los que se les han otorgado derechos de acceso pueden ver el documento.

Cuando se publica un documento de conocimiento, el usuario no suele tener permisos para modificar el documento a menos que se anule su publicación primero y después se puedan hacer modificaciones. Durante este tiempo, el documento de conocimiento está fuera de línea y no está disponible para los usuarios. El propietario del documento, un gestor de conocimientos, o un administrador del sistema no pueden publicar el documento mediante el botón Reproceso y la casilla de verificación Anular publicación. Al hacerlo, los documentos recobran el estado de borrador. Un usuario administrativo puede decidir el siguiente paso del proceso de workflow.

Control de versiones de documentos

Mediante las capacidades de control de versiones de documentos de Gestión del conocimiento, los analistas con privilegios de edición pueden crear una *versión borrador de reproceso* de un documento. Una versión de reproceso comienza como una copia del documento que se sustituye en la base de conocimiento después de verificarlo y volverlo a publicar. Se evita tener que anular la publicación del documento primero.

Los usuarios con privilegios de edición también pueden ejecutar las siguientes tareas de control de versiones:

- Guardar una versión de borrador de un documento.
- Revertir una versión a la anterior si surge un problema con la versión actual (Borrador o Publicado). En la ficha Versiones de la página Actualizar documento, los usuarios pueden seleccionar las diferentes versiones a la que desean revertir la versión actual para su reemplazo.
- Siga el número de las versiones del documento guardadas, suprimidas y archivadas en la base de conocimiento.

La bandeja de entrada de documentos de conocimiento del panel de resultados de CA Service Desk Manager es el repositorio de documentos en todos los estados, incluidos los documentos borrador guardados y asignados y los documentos borrador de reproceso.

Cómo gestionar versiones del documento

Los administradores pueden establecer y gestionar versiones del documento mediante la ejecución de los siguientes pasos:

1. Identificar quién puede editar documentos publicados y crear versiones borrador de reproceso. El rol que se utiliza para un registro de contacto en particular controla los privilegios de edición.
2. Definir una plantilla de proceso de aprobación que agrupará las tareas o los pasos que se deben completar durante el ciclo de vida del documento. De forma predeterminada, una plantilla de proceso de aprobación integrados permite a los usuarios crear documentos.
3. Determinar si se va a utilizar el proceso de aprobación del documento. Los analistas con permiso para omitir el proceso de aprobación pueden identificar las tareas con las que desean empezar al crear una versión borrador de reproceso.
4. Crear las reglas de archivo de archivado y el borrado definitivo para el mantenimiento de la versión del documento.

Vencimiento de documentos

Cuando un documento alcanza la fecha de vencimiento, normalmente el producto lo retira (es decir, elimina el documento de la base de conocimientos y del proceso de aprobación).

Archivado y borrado definitivo de documentos

Puede gestionar el tamaño de la agrupación de conocimiento mediante el archivado y borrado definitivo, que elimina automáticamente los documentos antiguos y sin utilizar. El archivado y el borrado definitivo mejora la eficacia de las búsquedas de conocimiento al devolver solamente los documentos actuales.

El archivado y borrado definitivo se ejecuta como un proceso en segundo plano y elimina automáticamente registros inactivos de la base de datos de CA Service Desk Manager según las reglas que se hayan configurado. Estas reglas actúan sobre los objetos de CA Service Desk Manager en intervalos de tiempo específicos.

Archivos de conocimiento

Un *archivo de conocimiento* es un archivo de texto que se puede buscar (.pdf, .zip, .xls, .exe, .html, .img, .msg, .ppt, .rtf, .txt, .avi, .doc y .xml), asociado con una categoría y que puede estar relacionado con otras categorías.

Los archivos de conocimiento son flexibles y permiten a los usuarios aprovechar rápidamente el conocimiento de un recurso exterior sin tener que volver a recomponer la información en un documento de conocimiento estructurado. Por ejemplo, un analista puede aprovechar el conocimiento de un distribuidor que explica cómo arreglar una impresora y guardarlo como un archivo de conocimiento en una categoría de conocimiento denominada "Impresoras".

Los usuarios pueden aprovechar de muchas maneras los archivos de conocimiento. Por ejemplo, pueden sustituir un archivo, convertirlo en un documento de conocimiento y descargar un archivo a otra ubicación. Las dos opciones de búsqueda, tradicional y avanzada, pueden utilizarse para buscar conocimiento dentro de un archivo.

Todos los archivos se almacenan en el repositorio de archivos de conocimiento, cuyo mantenimiento está a cargo del administrador para su seguridad y rápida recuperación.

Nota: Para obtener más información sobre cómo agregar archivos de conocimiento al repositorio, consulte la Biblioteca de adjuntos en la *Ayuda en línea*.

Búsqueda de conocimientos

Gestión del conocimiento proporciona a los usuarios las opciones siguientes para recuperar el conocimiento:

Exploración de categorías

Encuentra soluciones basadas en categorías. En cada categoría, las subcategorías adicionales pueden acotar los resultados de la búsqueda a un conjunto de soluciones que probablemente sean más relevantes para una incidencia.

Árbol de conocimiento

Realiza una serie de preguntas para guiar al usuario a las soluciones posibles. Las respuestas conducen al individuo a una solución que parece ser más relevante.

Marcador

Proporciona el acceso a documentos visualizados con más frecuencia que se incluyen en una lista de marcadores.

Foros

Los foros le permiten comunicarse acerca de las incidencias existentes. El uso de foros permite compartir documentos globalmente o entre grupos predefinidos que colaboran compartiendo conocimiento y debatiendo sobre los retos existentes.

Los foros amplían el ámbito de las contribuciones de conocimiento permitiendo el debate sobre cuestiones generales, consejos de uso, etc. El foro se puede crear en la ficha Conocimiento y desde un ticket del centro de servicio al usuario.

Documentos de árbol de conocimientos

El creador de árbol de conocimientos es una herramienta visual utilizada para crear árboles de conocimiento de una manera rápida y sencilla. Un árbol de conocimientos es una representación del conocimiento de expertos en un área determinada. En el creador de árbol de conocimientos, los analistas y los técnicos de conocimiento pueden crear árboles detallados que guían al usuario por una serie de preguntas y respuestas potenciales hasta alcanzar una resolución. Esta herramienta elimina la necesidad de habilidades de generación o programación de scripts especializadas y puede involucrar solamente el trabajo de un analista con un experto en la materia para crear un diseño de árbol.

Los árboles de conocimiento pueden tener un diseño complejo. Por lo tanto, antes de crear un árbol de conocimiento se recomienda construir un diagrama para asignar el diseño. El diagrama debe contener una serie de preguntas, posibles respuestas y resoluciones asociadas. La jerarquía de preguntas y respuestas del diagrama que se construye es la base en la que se crea el árbol de conocimiento.

Después de planear un diagrama del árbol de conocimiento, deberá construir el árbol utilizando el creador de árbol de conocimientos.

Programación de documentos de conocimiento

La programación de documentos de conocimiento proporciona a los gestores de cambio, gestores de conocimientos y analistas de nivel 2, una vista de alto nivel de los eventos clave en el ciclo de vida de gestión del conocimiento. En un documento de conocimiento se pueden programar los siguientes eventos:

- Envío
- Publicación
- Revisión
- Vencimiento

La ficha Programación de la gestión del conocimiento presenta un formato de calendario parecido al del calendario de cambios; pero, en lugar de mostrar horas de inicio y horas de finalización, únicamente muestra fechas específicas.

Las vistas de programación de configuración (see page 654) implican la programación de instrucciones de macros.

La programación del documento de conocimiento también se puede exportar al formato de iCalendar.

Nota: Al exportar las programaciones de ciertos programas de calendario, la selección de la opción Abrir en lugar de la opción Guardar genera una importación incorrecta del archivo. Para evitar esta incidencia en las programaciones de la gestión de conocimiento y de órdenes de cambio, seleccione la opción Guardar en lugar de Abrir. Después de guardar el archivo exportado, impórtelo a través de la interfaz del programa de calendario.

Filtro de programación del conocimiento

El filtro de programación del conocimiento muestra los siguientes campos:

Cliente

Filtra la búsqueda por cliente. Este campo muestra el usuario privilegiado en una instalación multicliente.

Tipo de evento

Filtra la búsqueda según los siguientes tipos de evento:

- Envío
- Revisión
- Publicación
- Retiro

Fecha de inicio de la programación

Especifica la fecha de inicio de un intervalo en el que filtrar el historial para mostrar solamente las entradas para un intervalo de tiempo especificado.

Programación de la fecha de finalización

Especifica la fecha de finalización de un intervalo en el que filtrar el historial para mostrar solamente las entradas para un intervalo de tiempo especificado.

Fecha horaria de la programación

Especifica una zona horaria para ver los resultados de la búsqueda.

Nota: Si no se selecciona ninguna zona horaria, los eventos se mostrarán en la zona horaria actual.

Propietario

Define el nombre del contacto asignado para realizar el mantenimiento del documento. Introduzca el nombre del contacto con el formato "apellidos, nombre" o abra el cuadro de diálogo Búsqueda de contactos para localizar y seleccionar un contacto.

Asignado

Especifica el nombre del contacto asignado para gestionar el registro. Introduzca el nombre del contacto con el formato "apellidos, nombre" o abra el cuadro de diálogo Búsqueda de contactos para localizar y seleccionar un contacto.

Experto

Define el nombre de un contacto con experiencia en el tema del documento. Introduzca el nombre del contacto con el formato "apellidos, nombre" o abra el cuadro de diálogo Búsqueda de contactos para localizar y seleccionar un contacto.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Para ejecutar la búsqueda, seleccione uno de los siguientes estados de documento:

- Borrador
- Publicado
- Retirado

Categoría

Define la categoría para filtrar los documentos recuperados. Introduzca el nombre de la categoría en el cuadro o abra la ventana Búsqueda de categorías. Al hacer clic en Buscar, el producto devuelve sólo los documentos asociados con la categoría especificada.

Vista inicial

Seleccione la vista del calendario de gestión de conocimiento que desea ver:

Mes

Muestra un calendario para el mes completo que incluye la fecha de inicio de implementación más antigua especificada en el campo Fecha de inicio. El calendario muestra información abreviada sobre cada cambio dentro del intervalo (el número de cambio, la hora de inicio y de finalización, y el primer CI afectado).

Semana

Muestra siete días consecutivos en una sola columna, empezando con la fecha de inicio de implementación más antigua especificada en el campo Fecha de inicio. El calendario incluye información de resumen sobre cada cambio dentro del intervalo especificado (el número de cambio, la hora de inicio y de finalización, la descripción resumida, el asignatario, el grupo y los primeros diez CI afectados).

Día

Muestra una vista similar a la vista de semana, con la diferencia de que muestra solamente el día especificado en el campo Fecha de inicio.

n días

Muestra una vista similar a la vista de semana, con la diferencia de que continúa para el número especificado de días.

Lista

Muestra una página de lista estándar de CA Service Desk Manager.

Nota: Puede hacer clic en el icono Más para mostrar el campo Argumentos de búsqueda adicionales. Este campo está dirigido únicamente a usuarios avanzados que comprenden SQL y Majic y que pueden usarlo para especificar argumentos de búsqueda que no están disponibles en los campos de filtros de búsqueda estándar. Puede introducir una cláusula WHERE de SQL en este campo para especificar un argumento de búsqueda adicional.

Vistas de programación de conocimiento

La programación de documentos de conocimiento tiene las siguientes vistas:

Mes

Muestra un calendario para el mes completo que incluye la fecha de inicio de implementación más antigua especificada en el campo Fecha de inicio de la programación. El calendario muestra información abreviada sobre cada cambio dentro del intervalo (el número de cambio, la hora de inicio y de finalización, y el primer CI afectado).

La programación de documentos de conocimiento tiene una funcionalidad semejante a la vista de mes de las órdenes de cambio con las excepciones siguientes:

- Los eventos de conocimiento sólo tienen fecha (no incluyen horas) y se agrupan por tipo de evento, de forma similar a las órdenes de cambio, que se agrupan por cada período de tiempo y tipo de cambio.
- Cuando se utilizan las macros de schedGroup, los tipos de eventos tienen los siguientes colores predefinidos predeterminados:
 - Envío: negro
 - Revisión: verde
 - Publicación: azul
 - Retiro: rojo

Nota: Si observa una fecha de revisión referida al pasado, esto puede indicar que no se ha efectuado la revisión.

Semana

Muestra siete días consecutivos en una sola columna, empezando con la fecha de inicio de implementación más antigua especificada en el campo Fecha de inicio de la programación. El calendario incluye información de resumen sobre cada cambio dentro del intervalo especificado (el número de cambio, la hora de inicio y de finalización, la descripción resumida, el asignatario, el grupo y los primeros diez CI afectados).

Día

Muestra una vista similar a la vista de semana, con la diferencia de que sólo el día especificado aparece en el campo Fecha de inicio de la programación.

n días

Muestra una vista similar a la vista de semana, con la diferencia de que continúa para el número especificado de días.

Lista

Muestra una página de lista estándar de CA Service Desk Manager.

Programación de la configuración de vista

Para configurar las vistas de programación mensual y semanal, especifique las declaraciones `pdm_macro` en la sección `<head>` de los formularios HTML que definen la programación. Se recomienda utilizar la vista de fuente de Web Screen Painter para modificar estos formularios.

Todos los formularios que muestran una programación deben incluir lo siguiente:

- Una macro `schedConfig`
- Una macro `schedAttr`, como mínimo
- Una macro `schedGroup`, como mínimo

Las macros de configuración se ubican en un archivo de origen separado al cual hace referencia la declaración `pdm_include` en un archivo de origen principal. Este archivo permite configurar la programación sin modificar el archivo de origen principal.

Por ejemplo, las macros de configuración para el formulario de calendario de cambios `list_chgsched.html` se encuentran en un archivo denominado `list_chgsched_config.html`. En la programación de ciclo de vida de conocimientos se puede modificar el archivo `list_kdsched_config.html` que utiliza las mismas macros.

Los archivos `list_chgsched_config.html` y `list_kdsched_config.html` se encuentran en el siguiente directorio:

```
$NX_ROOT\bopcfg\www\html\web\analyst\
```

Macro `schedConfig`: configurar programación

La macro `schedConfig` indica que un formulario contiene una programación y proporciona información de configuración básica. Los siguientes valores son argumentos de macro válidos:

`autosearch=1|0`

Especifica si el formulario de programación vuelve a cargar los datos del servidor cuando el usuario selecciona una vista fuera del intervalo de fechas actualmente seleccionado. Al establecer el valor en 1 (opción predeterminada), cuando el usuario selecciona una vista con uno o más días fuera del intervalo de selección de datos del filtro de búsqueda, el formulario realiza la búsqueda en forma automática. Al establecer el valor en 0, el usuario debe hacer clic en el botón Buscar para iniciar una búsqueda.

defaultView=0|1|7|30|99

Especifica la vista predeterminada para el filtro de búsqueda como 0 (lista), 1 (día), 7 (semana), 30 (mes) o 99 (día n).

La especificación de defaultView afecta solamente a la visualización inicial del filtro de búsqueda. Una vez que se muestra la programación, CA Service Desk Manager mantiene automáticamente la selección de la vista de filtro alineada con la vista actual.

Valor predeterminado: 30

firstday=0|1|2|3|4|5|6|7

Especifica el primer día laborable de la vista mensual como un número entre 0 (domingo) y seis (sábado).

Valor predeterminado: 0

export=xxx|0

Especifica el nombre del código de la plantilla utilizada para realizar la exportación en el formato iCalendar. Al establecer el valor en 0, la función de exportación y el botón Exportar quedan deshabilitados.

Valor predeterminado: ChangeSchedule

legend=1|2|0

Especifica la ubicación de la leyenda de la programación que muestra el nombre y el formato de los grupos de la programación. Puede establecer el valor en 1 para ubicar la leyenda por encima de la programación o en 2 para ubicar la leyenda por debajo de la programación. Puede establecer el valor en 0 para deshabilitar la leyenda.

Valor predeterminado: 2

maxGroups=0/n

Especifica el número máximo de grupos que se pueden mostrar en una sola celda de la vista mensual de calendario.

Si el número en el valor maxGroups programado para un solo día supera el máximo, CA Service Desk Manager muestra solamente el primer valor maxGroups-1 y reemplaza el último con un hipervínculo "..nn más cambios" sobre el cual el usuario puede pasar el ratón o hacer clic para ver la lista completa. Puede establecer el valor en 0 para deshabilitar esta función y permitir un número ilimitado de eventos en una celda del calendario.

Valor predeterminado: 4

nday=(n,n ...)

Especifica selecciones para la lista desplegable de la vista de día n.

La especificación es una lista de recuentos de los días que se van a incluir en la lista desplegable. El valor 0 se utiliza para indicar que la lista desplegable de día n se omite de la programación. El primer valor especificado es el valor predeterminado para la lista desplegable.

Valor predeterminado: (3,7,14,28)

round=(hr,min)|0

Especifica si las fechas de inicio y finalización de la programación se deben redondear al recopilar órdenes de cambio o documentos de conocimiento en grupos. Especifique round=0 para deshabilitar el redondeo.

De forma predeterminada, las fechas de inicio y finalización de la programación agrupan objetos. Todas las fechas de CA Service Desk Manager incluyen una hora, sin redondear, y los objetos programados a tan solo un minuto de diferencia se ubican en grupos separados. El redondeo determina el grupo después de ajustar la fecha de inicio a una hora o un minuto más temprano y la fecha de finalización a una hora o un minuto más tarde.

El valor de redondeo especifica una hora o un minuto (pero no ambos). Las horas se redondean al múltiplo más cercano del valor especificado, por ejemplo:

round=(0,15)	redondea al cuarto de hora más cercano
round=(0,30)	redondea a la media hora más cercana
round=1	redondea a la hora más cercana
round=12	redondea al medio día más cercano (0:00 ó 12:00)
round=24	redondea al día más cercano

Valor predeterminado: (0,15)

timefmt=24hr|([am],[pm])

Especifica el formato de las horas en las vistas de calendario de la programación.

El valor predeterminado 24hr indica que las horas se muestran en un formato de 24 horas (0:01 a 23:59). El valor alternativo (am,pm) especifica un sufijo para las horas de la mañana o de la tarde, o ambas.

Nota: Todos los argumentos schedConfig son opcionales.

Macro schedAttr: especificar un atributo almacenado

La macro schedAttr especifica un atributo almacenado para cada elemento que se selecciona de la lista. Los atributos almacenados están disponibles en la información que aparece al pasar el ratón por encima de la vista mensual, en la información detallada o de resumen de todas las vistas excepto la mensual y en la función setSchedEvents() de JavaScript. Los siguientes valores son argumentos de macro válidos:

attr=xxxx

(Obligatorio) Especifica un atributo de un objeto de la programación, como una orden de cambio o un documento de conocimiento. Se permiten atributos con puntos. El nombre de atributo de palabra clave *CInn* puede utilizarse en el calendario de cambios para especificar que las primeras *nn* clases asociadas con la orden de cambio están incluidas en la información almacenada.

Nota: Este argumento es el único argumento obligatorio de la macro schedAttr.

attrRef=.COMMON_NAME|xxxx

Almacena el atributo de la tabla almacenada para un atributo SREL (ignorado para los atributos que no sean SREL) a la que se hace referencia. El nombre del atributo especificado debe incluir un punto como prefijo.

Valor predeterminado: .COMMON_NAME

label=

Muestra una etiqueta para el atributo de la vista de día n.

Valor predeterminado: DISPLAY_NAME en Majic del atributo

ident=1|0

Especifica si el atributo es un identificador del objeto (como el número de referencia de una orden de cambio). Los atributos que funcionan como identificadores se muestran sin etiquetas delante del nombre de grupo en la información que aparece al pasar el ratón y en la vista de día n.

Valor predeterminado: 0

detail=1|0

Especifica si el atributo se incluye en la información de detalle que se muestra en vistas que no sean la vista mensual. La información de detalle es la que se muestra cuando la casilla de verificación Sólo resumen no está activada en la vista.

Valor predeterminado: 1

hoverInfo=1|0

Especifica si el atributo está incluido en el cuadro emergente con información que aparece en la vista mensual al pasar el puntero del ratón por encima de un grupo, o cuando el usuario pulsa las teclas Alt+Flecha derecha y el foco se encuentra sobre el grupo.

Valor predeterminado: 0

summary=1|0

Especifica si el atributo se incluye en la información de detalle que se muestra en vistas que no sean la vista mensual. La información de detalle es la que se muestra cuando la casilla de verificación Sólo resumen no está activada en la vista.

Valor predeterminado: 0

Nota: CA Service Desk Manager muestra los atributos en la información de resumen, la información detallada o la información que aparece al pasar el ratón en el mismo orden que muestra sus macros schedAttr.

Macro schedGroup: especificar un grupo de eventos

La macro schedGroup especifica la codificación de nombre y color de un grupo de elementos. La vista mensual reúne todos los elementos en un grupo dentro de un solo evento. Todas las vistas excepto la mensual muestran los elementos en forma individual en el formato del grupo al cual pertenecen. Los siguientes valores opcionales son argumentos de macro válidos:

grpname=xxx

(Obligatorio) Especifica el nombre del grupo. La macro automáticamente asigna un número al grupo y asigna el número a una variable de JavaScript con el nombre del formulario schedGroup_xxx, en el que xxx es el nombre del grupo. Esta variable se puede utilizar en la función setSchedEvents() de JavaScript para crear un evento que pertenezca al grupo.

Nota: Este argumento es el único argumento obligatorio de la macro schedGroup.

label=xxx

Especifica una etiqueta para el grupo. Si se especifica una etiqueta, ésta se muestra en todas las vistas.

legend=xxx|0

Muestra una descripción del grupo para la leyenda que aparece en la parte inferior de la programación. Los grupos aparecen en la leyenda si por lo menos un ejemplo del grupo existe en la vista actual. Si se especifica 0, el grupo se excluye de la leyenda.

Valor predeterminado: 0

color=black|color

Especifica el color del texto de los elementos de este grupo. Puede especificar el color en formato CSS, un color Web válido o un valor hexadecimal precedido por un signo de número.

Ejemplo: Introduzca "#FF0000" o "red" para rojo.

Valor predeterminado: negro

bgcolor=white|color

Especifica el color de fondo de los elementos de este grupo. Puede especificar el color de fondo en formato CSS, un color Web válido o un valor hexadecimal precedido por un signo numeral.

Ejemplo: Introduzca "#FF0000" o "red" para rojo.

Predeterminado: blanco.

style=normal|bold|italic

Especifica el estilo de texto de este grupo como normal, negrita o cursiva.

Valor predeterminado: normal

La función setSchedEvents() JavaScript

La función setSchedEvents() de JavaScript permite crear eventos en la programación. Modifique esta función cuando desee ver los objetos de cualquier grupo nuevo. Los objetos del grupo predefinidos aparecen de forma predeterminada.

CA Service Desk Manager invoca a la función setSchedEvents() una vez en relación con cada objeto (orden de cambio o documento de conocimiento) seleccionado por el filtro de búsqueda de la programación. Con el fin de crear eventos para el objeto, la función invoca a una segunda función, schedEvent(); y transfiere el ID de grupo, la fecha de inicio y la fecha de finalización del evento.

La función puede crear cualquier número de eventos (incluido cero) para un objeto. La función `setSchedEvents()` predeterminada para el calendario de cambios (`list_chgsched.html`) crea un evento para cada orden de cambio y agrupa estas órdenes por tipo de cambio. Esta función se codifica de la siguiente manera:

```
1.     función setSchedEvents( chg )
2.     {
3.     var grpnum;
4.     switch( chg["chgtype"] - 0) {
5.         caso 100: grpnum = schedGroup_std; break;
6.         caso 300: grpnum = schedGroup_std; break;
7.         predeterminado: grpnum = schedGroup_norm; break;
8.     }
9.     chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"]);
10.    }
```

El parámetro de caso especifica el ID del tipo de cambio. Para conocer cómo se enumeran los ID de caso, consulte [Creación de un tipo de cambio](#).

La función tiene un solo argumento perteneciente a un objeto de JavaScript que contiene los atributos que las macros `schedAttr` han especificado. La instrucción `switch` de las líneas 4-8 examina el atributo `chgtype` de la orden de cambio y asigna el número de grupo pertinente de una de las variables `schedGroup_xxxx` definidas por las macros `schedGroup` anteriores. En la línea 9, la instrucción invoca a la función `schedEvent()` para crear un evento en la programación mediante la transferencia del número de grupo previamente asignado y de las fechas de inicio y finalización de la programación. Las fechas están disponibles en el objeto del argumento, ya que se especificaron en las macros `schedAttr` anteriores.

Acceso a exportación/importación

La herramienta de exportación/importación de conocimiento migra y sincroniza los datos entre sistemas de Gestión del conocimiento diferentes y permite la exportación/importación de documentos de conocimiento. Utilice esta herramienta para definir transacciones de exportación/importación.

Nota: Si se instala el multicliente, todas las categorías de cliente y públicas que se importaron de un sistema anterior se muestran como públicas en el nuevo sistema multicliente, pero los documentos importados pueden ser específicos del cliente.

Para acceder a la página de KEIT, vaya a Conocimiento, Documentos, Exportar/importar en la ficha Administración.

Aparece la página de exportación/importación, que contiene los siguientes elementos:

Transacciones de exportación

Muestra una lista de exportaciones.

Exportar/importar plantillas

Muestra una lista de plantillas que se pueden editar.

Importar

Muestra una lista de paquetes disponibles para la importación.

Importar transacciones

Muestra una lista de importaciones.

Nota: Al importar o exportar conocimiento de la interfaz Web, Gestión del conocimiento utiliza el rol de utilidad de la línea de comandos predeterminado y no el rol actual con el que el usuario ha iniciado sesión en CA Service Desk Manager. Se establece el rol de utilidad de línea de comandos predeterminado en el tipo de acceso para el usuario.

Cómo exportar o importar conocimiento

Las plantillas de exportación/importación le permiten definir una transacción de exportación/importación.

Para exportar o importar conocimiento, realice los siguientes pasos:

1. Realice cualquiera de las siguientes acciones:
 - Crear una plantilla de exportación/importación para exportar un paquete.
 - Utilizar una plantilla de exportación/importación para exportar un paquete.
2. Exportar los datos a otro sistema mediante cualquiera de las siguientes acciones:
 - Haga clic en Exportar en la página Detalles de plantilla.
 - En la página Exportar transacciones, haga clic con el botón secundario en una transacción y haga clic en Reintentar en el menú contextual.
 - Uso de la utilidad pdm_ket (see page 811)

3. Permite importar datos de conocimiento del paquete mediante cualquiera de las siguientes acciones:
 - Copiar el paquete de conocimiento a una instalación de CA Service Desk Manager específica y colocarla en el directorio `$NX_ROOT/site/keit/import`.
 - En la página Lista de paquetes de importación de conocimiento, haga clic con el botón secundario en un paquete de conocimiento, y haga clic en Importar en el menú contextual.
 - En la página Importar transacciones, haga clic con el botón secundario en una transacción y haga clic en Reintentar en el menú contextual.
 - Uso de la utilidad `pdm_kit_txt` (see page 812)

Nota: El nombre del paquete de conocimiento debe comenzar con el prefijo "package_" para que aparezca en la página Importación de conocimiento.

Importante: la utilidad de importación de la versión r11.0 se ha renombrado a `pdm_kit_txt.exe` para permitir la importación de archivos de texto de la versión r11.0. Esta utilidad no admite ninguna de las mejoras de importación de la versión r12.0.

Más información:

[Paquetes de exportación/importación](#) (en la página 803)

Transacciones de exportación

Puede clasificar transacciones por paquete, plantilla y estado. Todas las transacciones de KEIT se registran en los siguientes archivos de registro:

stdlog

Registra información de CA Service Desk Manager.

keitstat.log

Proporciona información estadística sobre la operación de KEIT.

keitinfo.log

Proporciona información detallada sobre la operación de KEIT.

Nota: Si multicliente está instalado, la página de lista muestra la configuración de datos públicos y de clientes en el filtro de búsqueda. Los datos públicos se pueden excluir o incluir con los datos de clientes; sólo se buscan objetos públicos exclusivamente. En las páginas de detalles, seleccione el cliente apropiado de la lista. Si selecciona <vacío>, el objeto es público.

La página Exportar transacciones contiene los siguientes campos:

Paquete

Muestra el nombre del paquete de exportación.

Ejecutado por

Muestra el usuario que ejecutó la exportación.

Hora de inicio

Muestra la hora de inicio de la transacción.

Hora de finalización

Muestra la hora de finalización de la transacción.

Recuento de documentos

Muestra el número de documentos exportados.

Error de recuento

Muestra el número de exportaciones erróneas.

Progreso (%)

Muestra el progreso de la transacción.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Muestra el estado de la transacción.

Importar transacciones

La página Importar transacciones permite ordenar las transacciones por paquete, plantilla y estado al hacer clic en cualquiera de las columnas.

Nota: Si multicliente está instalado, la página de lista muestra la configuración de datos públicos y de clientes en el filtro de búsqueda. Los datos públicos se pueden excluir o incluir con los datos de clientes; sólo se buscan objetos públicos exclusivamente. En las páginas de detalles, seleccione el cliente apropiado de la lista. Si selecciona <vacío>, el objeto es público.

La página contiene los siguientes campos:

Paquete

Muestra el nombre del paquete de importación.

Ejecutado por

Muestra el usuario que ejecutó la importación.

Hora de inicio

Muestra la hora de inicio de la transacción.

Hora de finalización

Muestra la hora de finalización de la transacción.

Recuento de documentos

Muestra el número de documentos importados.

Error de recuento

Muestra el número de importaciones erróneas.

Progreso (%)

Muestra el progreso de la transacción.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Muestra el estado de la transacción.

Más información:

[Mostrar configuración de importación](#) (en la página 809)

Exportación e importación de documentos

Para migrar y sincronizar los datos entre diferentes sistemas de Gestión del conocimiento, utilice la herramienta de exportación/importación de conocimiento (KEIT) en Administración de conocimiento, que le permite exportar e importar documentos de conocimiento.

Puede crear plantillas de KEIT para definir una transacción de exportación/importación.

Nota: Para importar los datos de conocimiento de la versión r11.0, utilice la utilidad pdm_kit_txt.

Paquetes de exportación/importación

Los paquetes de exportación contienen la siguiente sintaxis:

- Nombre del servidor
- Date
- Hora de inicio

Puede definir directorios de paquetes editando la opción *keit_path* en Gestor de Opciones, Conocimiento. Los paquetes se almacenan en los directorios predeterminados siguientes:

- Paquetes de exportación
KEIT_PATH\export
- Importar paquetes
KEIT_PATH\import

Para agregar atributos para la disponibilidad de exportación/importación, agregue los siguientes nombres de atributo en el archivo NX.env:

@NX_KEIT_AVAILABLE_FIELDS

Agrega el nombre de atributo.

@NX_KET_ADDL_FIELDS

Agrega el nombre de atributo, y si el nuevo atributo es un SREL a otro objeto, agrega el nombre de atributo utilizado para sincronizar los sistemas de origen y destino.

Ejemplo: adición de atributos

```
@NX_KEIT_ADDL_FIELDS =  
STATUS_ID.STATUS,DOC_TEMPLATE_ID.TEMPLATE_NAME
```

Los directorios de exportación e importación contienen los siguientes archivos:

keit_config.xml

Contiene el archivo de configuración para un paquete de exportación o importación.

data.xml

Contiene el archivo de datos que incluye los valores de los documentos de conocimiento.

rep.xml

Contiene los repositorios a los cuales se hace referencia en el archivo data.xml.

images

Especifica los archivos de imagen incrustados en los documentos de conocimiento.

Visualización de plantillas de exportación/importación

Las plantillas de la Herramienta de importación/exportación de conocimiento (KEIT) se utilizan para definir transacciones de exportación/importación.

Nota: La plantilla de exportación/importación predeterminada se denomina Todos los documentos y no contiene el campo STATUS_ID. Esta plantilla crea el archivo data.xml e importa documentos con estado de borrador. Si agrega manualmente el campo STATUS_ID a la plantilla Todos los documentos antes de la operación de exportación, se conserva el estado del documento original en la importación.

Procedimiento para ver plantillas de exportación/importación de conocimiento

1. Haga clic en la ficha Administración.
Aparecerá la consola de administración.
2. Haga clic en Conocimiento, Documentos.
Haga clic en Exportar/importar, Exportar/importar plantillas.
Aparecerá la Lista de plantillas de exportación/importación de conocimiento.
3. Haga clic en una plantilla de la columna Nombre.
Se abre la plantilla de KEIT.

Nota: Puede exportar los resultados de la lista a Excel para su uso fuera de CA Service Desk Manager haciendo clic en el botón Exportar en la página de lista.

Búsqueda de plantillas de exportación e importación

Puede buscar una plantilla mediante la página de configuración de plantillas exportación/importación de conocimiento.

Nota: Si el multicliente está instalado, seleccione el cliente apropiado de la lista desplegable. La opción público (compartida) crea el objeto para todos los clientes. Aparece una lista desplegable de clientes en el filtro de búsqueda. Si selecciona <vacío> en esta lista desplegable, la búsqueda es pública. También aparece una columna de cliente en la página de lista.

Procedimiento para buscar plantillas de exportación/importación de conocimiento

1. En la ficha Administración, vaya a Conocimiento, Documentos, Exportar/importar, Exportar/importar plantillas.
Aparecerá la Lista de plantillas de exportación/importación de conocimiento.
2. Haga clic en Buscar e introduzca los parámetros de búsqueda.
Aparecerán los resultados de la búsqueda.
3. Haga clic en Mostrar filtro.
Aparecerá el filtro.
4. Modifique la búsqueda mediante las siguientes opciones:

Paquete

Busca por nombre de paquete.

Primera fecha de modificación

Busca por la fecha de la primera modificación.

Fecha de la última modificación

Busca por la fecha de la última modificación.

Argumentos de búsqueda adicionales

Proporciona argumentos de búsqueda adicionales.

Aparecerán los resultados de la búsqueda.

5. Haga clic en una plantilla en los resultados de la búsqueda.
Se abre la plantilla.

Creación de plantillas de exportación/importación

Puede crear y modificar una plantilla mediante la página de configuración de plantillas de exportación/importación de conocimiento en la ficha Administración.

Procedimiento para crear una plantilla de exportación/importación de conocimiento

1. En la ficha Administración, vaya a Conocimiento, Documentos, Exportar/importar, Exportar/importar plantillas.
Aparecerá la Lista de plantillas de exportación/importación de conocimiento.
2. Haga clic en Crear nuevo.
Aparece la página Crear nueva plantilla de exportación/importación.

3. Rellene los siguientes campos:

Nombre de plantilla

Identifica el nombre de la plantilla.

Descripción

Ofrece una descripción breve de la plantilla.

4. Rellene los campos pertinentes en las siguientes fichas:

- Exportar campos (see page 807)
- Exportar filtro (see page 808)
- Configuración de importación (see page 809)

Haga clic en Guardar.

La plantilla queda creada.

Véase también

[Transacciones de exportación](#) (en la página 801)

[Importar transacciones](#) (en la página 802)

Cómo mostrar campos de exportación

Para mostrar los campos de exportación, cree una plantilla de exportación/importación de conocimiento (KEIT).

Aparece la ficha Campos de exportación, que contiene los siguientes campos:

Disponible

Muestra los campos de los documentos de conocimiento que están disponibles para exportar.

Nota: Si desea preservar el estado de los documentos, como por ejemplo Borrador, durante el proceso de exportación e importación, agregue STATUS_ID a la columna Exportado.

Exportado

Especifica los campos de documento que se van a exportar.

Exportar archivos adjuntos

Exporta los archivos adjuntos de los documentos de conocimiento.

Puede utilizar las flechas de la sección Seleccionar atributos de documento para agregar atributos de documento a la exportación.

Nota: Si edita la plantilla de exportación/importación con Firefox, el tamaño de lista no se modifica después utilizar las flechas en la primera edición. Si la plantilla se cierra y vuelve a abrir en modo de edición, y se vuelven a utilizar las flechas, se producirán cambios en el tamaño de la lista. Este comportamiento no se produce al utilizar Internet Explorer.

Importante: los campos exportados en KEIT tienen una prioridad más alta que cuando se seleccionan como predeterminados en la ficha Importar configuración. Si selecciona un campo de exportación predeterminado en la ficha Importar configuración, no se procesa como campo predeterminado.

Cómo mostrar el filtro de exportación

Para mostrar el filtro de exportación, cree una plantilla de exportación/importación de conocimiento (KEIT).

Aparece la ficha Exportar filtro, que contiene los siguientes campos:

Categoría

Abre la página Categorías del conocimiento. Utilice esta opción para agregar categorías a la lista de la ficha Exportar filtro.

Eliminar categoría

Elimina las categorías de la lista de la ficha Exportar filtro.

Borrar categoría

Borra la lista de categorías de la ficha Exportar filtro.

Incluir categorías secundarias de las categorías

Exporta documentos a partir de las categorías secundarias de las categorías exportadas.

Incluir categorías secundarias

Exporta las categorías secundarias de los documentos exportados.

Incluir todos los documentos vinculados a las categorías seleccionadas

Exporta todos los documentos vinculados a las categorías seleccionadas.

Nota: Sólo está habilitado si se selecciona Incluir categorías secundarias.

Filtro adicional

Proporciona una cláusula WHERE adicional.

Mostrar configuración de importación

Para mostrar la configuración de importación, cree una plantilla de exportación/importación de conocimiento (KEIT).

Aparece la ficha Importar configuración, la cual contiene los siguientes campos:

Umbral de error (%):

Detiene el proceso de importación (establece el estado en Error) si el porcentaje de errores supera el número especificado.

Sustituir documentos publicados

Permite que los documentos importados sustituyan a los documentos publicados del servidor de destino.

Sustituir documentos en todos los estados no publicados

Permite que los documentos importados sustituyan a los documentos no publicados del servidor de destino.

Utilizar valores predeterminados cuando se sustituyen documentos

Utiliza valores predeterminados en los documentos sustituidos de campos definidos.

Indexar documentos inmediatamente

Indexa el documento tras el proceso de importación.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Seleccione Borrador, Publicado o Retirado.

Prioridad

Establece el nivel de prioridad de la configuración de importación.

Plantilla

Selecciona una de las siguientes plantillas predeterminadas:

- Documento de conocimiento integrado
- Árbol de conocimiento integrado
- Edición rápida integrada

Propietario

Permite establecer el propietario abriendo la página Búsqueda de contactos.

Autor

Permite establecer el autor abriendo la página Búsqueda de contactos.

Experto

Permite establecer el experto en la materia abriendo la página Búsqueda de contactos.

Asignado

Permite establecer el asignatario abriendo la página Búsqueda de contactos.

Fecha de vencimiento

Abre el asistente de fecha.

Fecha de revisión

Abre el asistente de fecha.

Product ID

Permite establecer el ID de producto abriendo la página Búsqueda de productos.

Activo

Abre la página Búsqueda de elementos de configuración.

Causa raíz

Abre la página Búsqueda de causas raíz.

Prioridad de Service Desk

Establece la prioridad de Service Desk de la configuración de importación.

Severidad

Establece el nivel de severidad de la configuración de importación.

Impacto

Establece el nivel de impacto de la configuración de importación.

Urgencia

Establece el nivel de urgencia de la configuración de importación.

Edición de una plantilla de exportación/importación

Puede editar las plantillas de exportación e importación desde la página Lista de plantillas de exportación/importación de conocimiento.

Para editar una plantilla de exportación o importación

1. Vaya a Conocimiento, Documentos, Exportar/importar, Exportar/importar plantillas.

Aparecerá la Lista de plantillas de exportación/importación de conocimiento.

2. Seleccione una plantilla.

Aparecerá la página Detalles de plantilla.

3. Haga clic en Editar.

Modifique los campos apropiados:

Nombre de plantilla

Identifica el nombre de la plantilla.

Descripción

Ofrece una descripción breve de la plantilla.

4. Modifique los campos apropiados en las siguientes fichas:

- Exportar campos (see page 807)
- Exportar filtro (see page 808)
- Configuración de importación (see page 809)

5. Haga clic en Guardar.

Se guardarán las ediciones.

Más información:

[Importar transacciones](#) (en la página 802)

Herramienta de exportación de conocimiento de utilidad de pdm_ket

La utilidad pdm_ket exporta el conocimiento a un paquete de conocimiento, en función de una plantilla creada desde la interfaz Web de un equipo de origen.

Los adjuntos y sus vínculos se exportan a data.xml durante la exportación. Antes de importar los adjuntos, muévelos manualmente al siguiente directorio del servidor de destino:

\$NX_ROOT/site/attachments/default

Utilice esta utilidad para hacer lo siguiente:

- Crear el archivo de configuración en función de la plantilla de exportación de conocimiento relacionada.
- Exportar los datos con el UUID de documento, y el contenido, como por ejemplo título, resumen, problema, resolución y otros atributos de documento como propietario, estado, etc.
- Exportar todas las imágenes exclusivas utilizadas por los documentos exportados (siempre se exportan).
- Exportar todos los adjuntos exclusivos utilizados por los documentos exportados (campo de EXP_ATTMENT).

Los archivos se copian desde el repositorio remoto a la carpeta del paquete local.

La utilidad se invoca de la siguiente manera:

```
pdm_ket -n <nombre de plantilla> [-h] [-v]
```

-n <nombre de plantilla>

Define el nombre de la plantilla utilizada para la exportación (distingue entre mayúsculas y minúsculas).

-h

(Opcional) Muestra la ayuda en la utilidad.

-v

(Opcional) Habilita el registro extenso (bop_logging) de los eventos de programas. Esta opción suele usarse para resolver problemas internos.

Ejemplo: utilización de pdm_ket para exportar conocimiento utilizando la plantilla mi_plantilla.

```
pdm_ket -n mi_plantilla
```

La utilidad pdm_ket se puede programar mediante un programador de terceros para exportar los documentos de conocimiento.

Utilidad pdm_kit: herramienta de importación de conocimiento

La utilidad pdm_kit importa los datos para el servidor de destino según las definiciones del archivo de configuración de un paquete.

Importante: la utilidad de importación de la versión r11.0 se ha renombrado a pdm_kit_txt.exe para permitir la importación de archivos de texto de la versión r11.0. Esta utilidad no admite ninguna de las mejoras de importación de la versión r12.5.

Los datos con referencias a los que la utilidad `pdm_kit` hizo referencia obtienen el valor de UUID o de ID del servidor de destino. Al ejecutar la utilidad `pdm_kit` se aplica un nuevo parámetro `userid`. La utilidad `pdm_kit` funciona de la siguiente manera:

1. Importa los documentos reemplazando el valor de `userid` (para los contactos) o del nombre al que se hace referencia (para campos como activo) con el UUID apropiado del servidor de destino.
2. Importa las imágenes.
3. Importa los archivos adjuntos.
4. Carga los archivos de la carpeta del paquete local en los repositorios remotos.

Nota: Si la edición de documentos publicados está desactivada, el documento importado se crea como una nueva versión de reproceso.

La utilidad se invoca de la siguiente manera:

```
pdm_kit [-h] -f -u [-v]
```

-h

(Opcional) Muestra la ayuda de la utilidad en la interfaz.

-f

Especifica la ruta para el paquete

-u

Especifica el usuario predeterminado.

-v

(Opcional) Habilita el registro extenso (`bop_logging`) de los eventos de programas. Esta opción suele usarse para resolver problemas internos.

Ejemplo: utilización de `pdm_kit` para importar un paquete

```
pdm_kit -f c:\ruta_paquete -u ServiceDesk
```

Cómo permitir a los usuarios exportar e importar conocimiento

Puede permitir a los analistas conceder permisos de exportación e importación mediante la gestión de la lista de roles en la ficha Administración.

Procedimientos para conceder permisos de exportación/importación

1. Vaya a Gestión de roles y seguridad, Gestión de roles, Lista de roles.
Aparecerá la lista de roles.
2. Seleccione un rol con el tipo de interfaz Analista.
Aparecerá la página Detalles del rol.
3. Haga clic en Editar.
Aparecerá la página Actualizar rol.
4. Haga clic en la ficha Conocimiento.
Realice cualquiera de las siguientes acciones:
 - Active la casilla de verificación Permitir exportación.
 - Active la casilla de verificación Permitir importación.
 - Active ambas casillas de verificación.
5. Haga clic en Guardar.
Volverá a aparecer la página Detalles del rol.
6. Revise los cambios en la ficha Conocimiento.
Cierre la página Detalles del rol.

También puede restringir la exportación/importación para los usuarios desactivando las casillas de verificación en la ficha Conocimiento de la página Detalles del rol.

Servicios Web

Se puede acceder al conocimiento a través de los servicios Web. Hay varios métodos disponibles que permiten buscar, recuperar, crear y actualizar documentos, así como muchas otras operaciones.

Nota: Para obtener más información sobre los servicios Web, consulte la *Guía de implementación*.

Capítulo 20: Administración de Gestión del conocimiento

Esta sección contiene los siguientes temas:

[Administración de conocimientos](#) (en la página 815)
[Búsqueda de procedimientos para la administración de conocimiento](#) (en la página 816)
[Funciones y roles de Gestión del conocimiento](#) (en la página 816)
[Cómo gestionar los privilegios de rol y la visibilidad del documento](#) (en la página 829)
[Contenido de acción](#) (en la página 830)
[Proceso de aprobación del documento](#) (en la página 835)
[Políticas automatizadas](#) (en la página 842)
[Control del documento de conocimiento](#) (en la página 847)
[Categorías de conocimientos](#) (en la página 863)
[Informes y métricas](#) (en la página 873)
[Búsqueda](#) (en la página 875)
[Opciones de integración de CA Service Desk Manager](#) (en la página 898)
[Solution Survey](#) (en la página 907)
[Configuración del sistema de Gestión del conocimiento](#) (en la página 910)

Administración de conocimientos

Puede configurar valores administrativos para Gestión del conocimiento. Puede definir opciones de conocimiento de autoservicio (see page 819) para satisfacer las necesidades de los usuarios y crear un entorno eficaz y efectivo de gestión y entrega del conocimiento. La ficha Administración le permite establecer las opciones del sistema. Puede establecer permisos de conocimiento basados en el grupo o rol de un contacto. La aplicación de la configuración contribuye a ajustarse a la funcionalidad y el uso de Gestión del conocimiento.

Importante: la reindexación de los documentos de la base de conocimiento y la ejecución del cálculo para las políticas automatizadas y la tarjeta de informes de conocimiento puede requerir mucho tiempo. Recomendamos que estas operaciones se ejecuten durante un horario no laboral o cuando el sistema esté menos ocupado.

Búsqueda de procedimientos para la administración de conocimiento

CA Service Desk Manager proporciona procedimientos detallados para la administración de conocimiento en esta guía y en la *Ayuda en línea*.

Para encontrar procedimientos detallados para la administración de conocimiento en la *Ayuda en línea*

1. Inicie sesión en CA Service Desk Manager.
Aparecerá la página principal de CA Service Desk Manager.
2. Realice alguna de las siguientes acciones:
 - Haga clic en Ayuda, Ayuda en el menú principal y vaya a la *Ayuda en línea* en Administración, Administración de conocimiento.
Aparecen los temas de Administración de Conocimiento y puede desplazarse por la jerarquía para encontrar la información que desee.
 - Haga clic en Ayuda, Ayuda acerca de esta ventana en el menú principal.
Aparece la *ayuda en línea* y muestra un tema de ayuda para la página acerca de la cual desea información.

Funciones y roles de Gestión del conocimiento

Gestión del conocimiento está diseñado para diversos usuarios, desde administradores y gestores de conocimientos, que se ocupan del mantenimiento del producto para los clientes, hasta empleados, que utilizan el sistema para encontrar soluciones a sus problemas. Aunque una persona puede desempeñar varios roles, los siguientes son los roles de usuario básicos en Gestión del conocimiento:

- **Cliente:** usuario final externo que realiza tareas básicas de autoservicio.
- **Empleado:** usuario final interno que realiza tareas básicas de autoservicio.
- **Analista de conocimiento:** usuario responsable de uno o más pasos en el proceso de gestión de conocimiento. Este usuario interactúa con los analistas de Service Desk para crear y mantener una base de solución de calidad.

- **Gestor de conocimientos:** supervisor para el analista de conocimiento. Este rol trata las escalaciones y reasignaciones del documento de conocimiento, y gestiona los aspectos administrativos diarios de la solución, incluida la creación de la estructura de categoría, la definición del proceso de aprobación, la gestión de las palabras irrelevantes, los términos especiales, los sinónimos y otras configuraciones y opciones más dinámicas que los controles del administrador de gestión del conocimiento.
- **Administrador:** administrador que tiene acceso a todas las funcionalidades en los productos de CA Service Desk Manager y Gestión del conocimiento dentro de un solo rol. Este rol se suele utilizar al implementar CA Service Desk Manager para contribuir a garantizar que todos los usuarios y roles están configurados correctamente y para un entorno de CA Service Desk Manager con una sola persona que realiza todas las tareas de administración.
- **Administrador de Gestión del conocimiento:** administrador responsable de configurar y controlar el proceso de gestión del conocimiento. Este rol incluye la creación de la estructura de categorías, la definición del proceso de aprobación y la configuración de los valores predeterminados de búsqueda y seguridad.

Se asocian diferentes niveles de acceso con cada rol en el entorno de CA Service Desk Manager. Estos niveles ayudan a definir las tareas que cada rol realiza.

Véase también

[Interfaces de usuario de Gestión del conocimiento](#) (en la página 818)

[Funciones de gestión y configuración de Gestión del conocimiento](#) (en la página 818)

[Opciones de conocimiento de autoservicio](#) (en la página 819)

[Documentos y usuarios](#) (en la página 825)

[Cómo gestionar los privilegios de rol y la visibilidad del documento](#) (en la página 829)

Interfaces de usuario de Gestión del conocimiento

Las siguientes interfaces de usuario le ayudarán a gestionar el conocimiento:

- **Autoservicio:** En la interfaz de autoservicio, los clientes y los empleados que utilizan CA Service Desk Manager pueden tener acceso a los documentos de conocimiento y enviar conocimientos para seguirlos estudiando. Los clientes pueden buscar, examinar o utilizar marcadores para localizar y ver documentos de conocimiento.
- **Documentos de conocimiento:** En la interfaz de documentos de conocimiento, a la que se puede acceder desde el nodo Documentos de conocimiento en el panel de resultados de CA Service Desk Manager, todos los usuarios del sistema pueden ver su Bandeja de entrada y comentarios de seguimiento. El *administrador* gestiona documentos sin asignar y sin indexar, políticas del ciclo de vida de documentos automatizados y foros de usuario.
- **Gestión del conocimiento:** En la interfaz de gestión del conocimiento, a la que se puede tener acceso en la ficha Conocimiento de CA Service Desk Manager, el *analista de conocimiento* o el *gestor de conocimientos* pueden encontrar, organizar y publicar el conocimiento. También pueden filtrar los documentos mostrados utilizando opciones avanzadas y clasificar los resultados en función de su relevancia, fecha de modificación y mucho más.
- **Administración de conocimiento:** En la interfaz de administración de conocimiento, a la que se puede tener acceso desde el nodo Conocimiento en la ficha Administración de CA Service Desk Manager, el *administrador*, *gestor de conocimientos*, o *administrador de gestión del conocimiento* pueden fijar las opciones del sistema. La configuración permite ajustarse a la funcionalidad y el uso de Gestión del conocimiento.

Funciones de gestión y configuración de Gestión del conocimiento

En Gestión del conocimiento, se pueden ejecutar las siguientes funciones de configuración y gestión:

- Crear "contenido de acción" (una URL de acción en vivo) que se puede insertar en el campo Resolución de un documento.
- Configurar el proceso de aprobación y definir el proceso del ciclo de vida del documento de conocimiento.
- Crear políticas automatizadas que automatizan determinadas tareas en el proceso de aprobación del documento de conocimiento.
- Configurar las opciones de documentos relacionadas con los comentarios, el envío de conocimiento, las plantillas y los valores de documento.
- Crear plantillas que controlan el modo en que un documento muestra la información.

- Gestionar el motor de búsqueda de Gestión del conocimiento predeterminado y configurar las palabras irrelevantes, los términos especiales y los sinónimos empleados para realizar búsquedas por palabras clave y por lenguaje natural.
- Si CA Service Desk Manager se ha configurado para utilizar el motor de búsqueda de Gestión del conocimiento, se puede cambiar al motor de búsqueda FAST opcional (si está instalado). El motor de búsqueda FAST proporciona capacidades de búsqueda adicionales que permiten buscar soluciones de conocimiento mediante un sitio Web o un sistema de archivos, y mucho más.
- Crear "documentos recomendados" que se muestran en la interfaz de autoservicio cuando los usuarios buscan soluciones de conocimiento.
- Los tickets de búsqueda utilizan la funcionalidad Buscar similar. Se requiere el motor de búsquedas FAST ESP.
- Gestionar la estructura de categorías de conocimientos para facilitar el acceso a los documentos.
- Configurar la tarjeta de informes de conocimiento y los valores generales del sistema.
- Definir encuestas que recopilan y analizan la opinión de los clientes sobre el rendimiento del documento de conocimiento.
- Gestionar la integración de Gestión del conocimiento en CA Service Desk Manager, incluida la asignación de campos y la configuración de búsqueda de solicitudes e incidencias.

Opciones de conocimiento de autoservicio

Los clientes y empleados que utilizan CA Service Desk Manager tienen acceso a los documentos de conocimiento a través de la interfaz de autoservicio. Los clientes pueden buscar, examinar o utilizar marcadores para localizar y ver documentos de conocimiento. Cuando se concede a los clientes el acceso a los documentos de conocimiento y los servicios, ellos pueden encontrar respuestas por sí mismos y se reduce la presión sobre los recursos.

En la interfaz de usuario de autoservicio, los empleados y los clientes pueden ver las siguientes opciones de soluciones de conocimientos:

- **Búsqueda de soluciones de conocimientos:** Los empleados y los clientes pueden escribir frases y palabras clave en un campo de búsqueda que permiten recuperar una lista de soluciones de conocimiento. Puede configurar esta opción en la siguiente ubicación: Administración, Conocimiento, Buscar, Valores de búsqueda.

- **Visualización de las mejores soluciones:** Los empleados y los clientes pueden mostrar una lista de las mejores soluciones en la interfaz de autoservicio. La siguiente configuración del administrador: Administración, Conocimiento, Sistema, Valores generales, Mejores soluciones: número de documentos que se van a mostrar, determina el número de documentos que se va a mostrar.
- **Mensaje para la encuesta de conocimientos:** Después de abrir un documento de conocimiento, el usuario puede leer el documento y acceder a una serie de preguntas de la encuesta. Una de estas preguntas permite al cliente indicar mediante un mensaje si cree que su problema ha sido resuelto. Puede configurar esta opción en la siguiente ubicación: Administración, Conocimiento, Encuesta de soluciones, Valores de la encuesta.
- **Sugerir conocimiento:** los empleados y clientes pueden, si se les permite, ver una lista de sugerencias de conocimiento cuando crean un ticket en la interfaz de autoservicio. Puede configurar esta opción en la siguiente ubicación: Administración, Conocimiento, Integración de Service Desk, Sugerir conocimiento.

Búsqueda avanzada

En Valores de búsqueda avanzada, los clientes y los empleados pueden utilizar las opciones siguientes para definir mejor una búsqueda de la solución de un problema:

Búsqueda de Gestión del conocimiento

Busca determinadas palabras clave, que sirven como coincidencias preliminares.

Búsqueda por lenguaje natural

Busca palabras y tiene en cuenta la proximidad y el orden de las palabras y la relevancia.

Los resultados de la búsqueda se muestran por la relevancia. Cada resultado puede incluir un título que aparece como un vínculo, un resumen del documento y estadísticas adicionales relevantes para éste, como por ejemplo la valoración de relevancia, el ID de documento, la fecha de modificación, la clasificación de preguntas frecuentes y las coincidencias recibidas. Según el modo en que el administrador del sistema haya configurado Gestión del conocimiento, los usuarios podrán abrir un incidente, valorar un documento y proporcionar comentarios cuando se abra un documento de conocimiento.

Información de documentos de conocimiento

Cada documento de conocimiento contiene campos de documento clave que brindan información. Según la plantilla de documento utilizada, aparecen campos diferentes, o aparecen de manera diferente en el documento.

El documento se identifica con un título. El documento también incluye la siguiente información:

Resumen

Resume el documento y describe brevemente el problema.

Problema

Describe el problema.

Resolución

Describe cómo resolver el problema en texto sin formato o en formato HTML.

Véase también

Se muestran los documentos relacionados con el documento actual. Al hacer clic en un hipervínculo del documento, se abre una página independiente que contiene el documento relacionado.

Adjuntos

Se muestran los archivos que se adjuntan al documento y que se pueden descargar. Los adjuntos proporcionan información adicional sobre el documento.

Categorías relacionadas

Se muestran las categorías relacionadas con el documento. Si hace clic en el hipervínculo de una categoría, se actualiza la página Herramientas de búsqueda para mostrar esa categoría.

Tickets relacionados

Vínculos a solicitudes, incidentes, problemas, incidencias y documentos que se han abierto como resultado del documento o que se han resuelto mediante el documento.

Propiedades

Indica las propiedades de documento adicionales seleccionadas en la plantilla de documento. De forma predeterminada, se muestran la fecha de modificación y el ID de documento.

Comentarios

Se muestran los comentarios de los usuarios para el documento. Junto con los comentarios se incluyen el nombre de contacto, la dirección de correo electrónico y la fecha.

Clasificación y comentario

Proporciona comentarios de seguimiento y evaluación que indican si el documento ha sido útil a la hora de responder a la pregunta. Permite valorar la utilidad del documento basándose en las siguientes preguntas:

- ¿Ha resuelto este documento su problema?
- ¿Resultó útil este foro?

También es posible agregar un comentario y asignárselo a otro analista para que realice el seguimiento, utilizando alguno de los tipos de comentario siguientes:

- Vínculo roto
- Candidato para publicación
- Candidato para retiro
- Información incorrecta
- Información que falta
- Recomendar contenido nuevo
- Revisión
- La solución no funciona

La sección Opciones de página permite realizar las siguientes acciones:

- Editar
- Agregar/Eliminar marcador
- Suscribir
- Clasificación y comentario
- Correo electrónico
- Nuevo foro
- Nuevo incidente
- Nuevo incidente basado en este documento
- Versión para imprimir

Más información:

[Creación de tipos de comentario](#) (en la página 850)

[Configuración de políticas de autoservicio](#) (en la página 907)

Anuncios

Los anuncios son una forma rápida de proporcionar soluciones para un problema. Los anuncios proporcionan una solución para un problema amplio y responder para responder las llamadas al centro de servicio al usuario.

Los anuncios actuales se muestran en el panel derecho de la ventana principal de CA Service Desk Manager, la primera vez que se inicia sesión en el sistema.

Clasificación de documentos

Los documentos se pueden clasificar en distinto orden.

Procedimiento para clasificar documentos

1. En la ficha Conocimiento, seleccione un nodo de árbol de la lista de categorías situada en el panel izquierdo.
2. Despliegue el nodo y haga clic en una categoría.
Aparecerá la página Lista de documentos.
3. Clasifique los documentos utilizando la lista Ordenar por, según el siguiente orden:
 - clasificación de preguntas frecuentes
 - Número de coincidencias
 - Documentos modificados recientemente
 - Recuento de soluciones

Los documentos se muestran en el orden seleccionado.

Exploración de documentos

Los documentos de conocimiento se pueden clasificar para permitir a los clientes examinar la información según las preguntas más frecuentes (FAQ). Al seleccionar una categoría de conocimiento, aparecen las subcategorías y los documentos de conocimiento relacionados. Puede seleccionar el documento que le gustaría ver, o seleccionar una subcategoría para acotar aún más la búsqueda.

Para mejorar las capacidades de autoservicio, aparece una lista dinámica de los documentos utilizados con mayor frecuencia.

Nota: Los usuarios de CA Service Desk Manager pueden especificar criterios sobre un elemento de interés y el motor de búsqueda busca los documentos de conocimiento coincidentes y los muestra en la página de resultados de la búsqueda como un conjunto de vínculos de "documentos recomendados". La consulta de búsqueda se puede expresar como una palabra clave o conjunto de palabras (frase) que identifica el concepto deseado que pueden contener uno o varios documentos. Para obtener más información, consulte Creación de nuevos documentos recomendados (see page 893).

Marcado de documentos

Se pueden marcar los documentos a los que se accede con mayor frecuencia. Después de que un documento ha sido marcado, se agrega a la lista Marcador. Esta lista le ayuda a localizar los documentos con más rapidez que la que normalmente se observa. Después de agregar un documento a una lista de marcadores, aparece un botón Eliminar en el campo Marcador. Puede quitar los marcadores de la lista cuando ya no se acceden con frecuencia.

La carpeta Mis marcadores almacena los vínculos a los documentos de referencia utilizados con más frecuencia. Al hacer clic en Mis marcadores en el panel Categoría de la ficha Conocimiento, la lista de documentos marcados aparece en el panel Lista de documentos de conocimientos.

Incidentes y problemas

Algunas veces los clientes tienen problemas que no se pueden resolver sencillamente realizando búsquedas de conocimiento. No todos los problemas tienen una solución directa en la base de conocimiento. Cuando un cliente tiene un problema que no se puede resolver, puede crear un incidente que se envía a un analista para el procesamiento posterior. El incidente describe el problema y, además, se puede basar en un documento de conocimiento existente. Cuando más información se agregue a un incidente, más fácil será para el analista su resolución.

Muchas actividades definidas por ITIL se admiten en Gestión del conocimiento, incluidas las siguientes:

- Gestión de incidentes
 - Las búsquedas de conocimientos pueden ayudar a encontrar errores conocidos durante la posterior investigación y diagnóstico del incidente
 - Categorización del incidente

- Gestión de problemas
 - Acceso a información sobre errores conocidos y ayuda en la coincidencia de problemas para obtener la resolución en los casos en que el problema ha ocurrido anteriormente
 - Acceso a información sobre soluciones temporales y mantenimiento de dicha información
 - Registro de información sobre procedimientos, instrucciones de trabajo, scripts de diagnósticos y errores conocidos (mientras se mantiene el soporte para contenido enriquecido, las herramientas de edición, las mediciones y un proceso de aprobación para el desarrollo de resoluciones que se pueda definir)
 - Análisis de problemas (mediante la vinculación y el análisis de incidentes)

Documentos y usuarios

En la interfaz de documentos de conocimiento, a la que se puede acceder desde el nodo Documentos de conocimiento en el panel de resultados de CA Service Desk Manager, todos los usuarios del sistema pueden ver su Bandeja de entrada y comentarios de seguimiento. El administrador gestiona documentos sin asignar y sin indexar, políticas del ciclo de vida de documentos automatizados y foros de usuario.

Bandeja de entrada de documentos

La bandeja de entrada de documentos de conocimiento (y la bandeja de entrada de grupo) del panel de resultados de CA Service Desk Manager contiene los documentos que se asignan al usuario o a un grupo. Es el repositorio central de documentos en todos los estados, incluidos los documentos borrador guardados y asignados y los documentos borrador de reproceso.

La bandeja de entrada es el contenedor de tareas cotidiano, una herramienta importante para gestionar el proceso de aprobación. Cuando se crea o actualiza un documento, se coloca en la bandeja de entrada de un propietario. Los elementos que aparecen en la Bandeja de entrada requieren la atención del usuario como parte del proceso de publicación. Hasta que se publican, los elementos de la Bandeja de entrada pueden no parecer resoluciones y no se agregan a la base de conocimiento. Controle periódicamente la bandeja de entrada para determinar si aparecen nuevos documentos.

Cómo mostrar comentarios de seguimiento

La bandeja de entrada de comentarios de seguimiento en el panel de resultados de los documentos de conocimiento de CA Service Desk Manager contiene los comentarios asignados al usuario o grupo.

En la página Lista de comentarios puede ver información resumida de los comentarios de seguimiento que se le han asignado.

Para mostrar los comentarios de seguimiento, vaya a Documentos de conocimiento, Comentarios de seguimiento.

Atributos de Documento

Establecer los atributos de documento ayuda a gestionar los documentos en la agrupación de conocimiento. Los atributos de documento se pueden actualizar para asignar al documento un experto en la materia o propietario nuevos. También se puede especificar la fecha en que el documento estará disponible en la base de conocimiento y la fecha en que caduca. Al seleccionar plantillas de documento diferentes, puede modificar el aspecto de cada documento.

Permisos del documento

Puede establecer, ver y editar los permisos para un documento. Estos permisos se pueden asignar a diferentes grupos de individuos. Al establecer permisos, se puede decidir heredar permisos de la categoría principal de un documento o especificar nuevos permisos. De forma predeterminada, los documentos heredan los permisos de su categoría principal. Este valor predeterminado controla los permisos de acceso a nivel de la categoría en vez de hacerlo a nivel del documento.

Importante: al crear un documento de conocimiento, verifique que los permisos del documento incluyan los usuarios que más tarde pueden estar asignados en el documento mediante el proceso de aprobación. Cuando se asigna un grupo a un documento, los usuarios de ese grupo pueden no disponer de permiso para ver el documento. Si el documento está asignado a un usuario específico, las restricciones de partición de datos predeterminadas permiten al usuario ver el documento.

Categorías de conocimientos

Asigne cada documento a una categoría primaria. Por ejemplo, cualquier conocimiento relacionado con Microsoft Word se debe agregar a la categoría de Microsoft Word. Además, Gestión del conocimiento permite asociar un documento con varias categorías secundarias y otros documentos. De esta manera, un documento se puede clasificar en distintas categorías aplicables y puede proporcionar resultados de búsqueda más satisfactorios. Después de crear un vínculo de documento, aparece un vínculo *Ver también* cuando se visualiza cualquiera de los documentos vinculados. El vínculo *Ver también* permite ir directamente de un documento vinculado a otro.

Archivos de conocimiento

Un *archivo de conocimiento* es un archivo de texto que se puede buscar (.pdf, .zip, .xls, .exe, .html, .img, .msg, .ppt, .rtf, .txt, .avi, .doc y .xml), asociado con una categoría y que puede estar relacionado con otras categorías.

Los archivos de conocimiento son flexibles y permiten a los usuarios aprovechar rápidamente el conocimiento de un recurso exterior sin tener que volver a recomponer la información en un documento de conocimiento estructurado. Por ejemplo, un analista puede aprovechar el conocimiento de un distribuidor que explica cómo arreglar una impresora y guardarlo como un archivo de conocimiento en una categoría de conocimiento denominada "Impresoras".

Los usuarios pueden aprovechar de muchas maneras los archivos de conocimiento. Por ejemplo, pueden sustituir un archivo, convertirlo en un documento de conocimiento y descargar un archivo a otra ubicación. Las dos opciones de búsqueda, tradicional y avanzada, pueden utilizarse para buscar conocimiento dentro de un archivo.

Todos los archivos se almacenan en el repositorio de archivos de conocimiento, cuyo mantenimiento está a cargo del administrador para su seguridad y rápida recuperación.

Nota: Para obtener más información sobre cómo agregar archivos de conocimiento al repositorio, consulte la Biblioteca de adjuntos en la *Ayuda en línea*.

Permisos de adjuntos

Los permisos de adjuntos se pueden gestionar en Biblioteca de adjuntos, en el nodo Repositorios de la ficha Administración. Los permisos de la carpeta de repositorio se pueden configurar según las necesidades de la compañía.

Nota: Un documento puede tener permisos diferentes que sus adjuntos vinculados.

Cómo agregar adjuntos de documentos

Al trabajar con documentos de conocimiento, puede adjuntar archivos o direcciones URL complementarios a los documentos. Estos archivos o direcciones URL complementarios proporcionan acceso fácil a información adicional relacionada con los documentos de conocimiento. Los archivos adjuntos se almacenan en un repositorio.

Utilice la ficha Adjuntos para gestionar las direcciones URL y los archivos adjuntos en el documento actual. En los documentos creados mediante las plantillas Documento de conocimiento integrado o Árbol de conocimiento integrado, los vínculos a los archivos adjuntos se muestran en el encabezado Adjuntos.

Nota: La ficha Adjuntos muestra solamente los documentos publicados. En el caso de los documentos no publicados, la ficha Adjuntos muestra los paneles Repositorios, Archivos y Adjuntos, y una lista de direcciones URL y de archivos actualmente adjuntados al documento.

Procedimiento para agregar un archivo adjunto a un documento

1. Abra el documento para editarlo.
2. Haga clic en la ficha Adjuntos.
3. Introduzca la URL que desee adjuntar.
4. Realice uno de los procedimientos siguientes:
 - Haga clic en Adjuntar archivo para agregar un archivo de su sistema.
 - Haga clic en Adjuntar archivo de la biblioteca para seleccionar el nombre de archivo que desea adjuntar de la lista Repositorios.

El nombre se muestra en la ficha Adjuntos.

Nota: Si copia un documento con uno o varios adjuntos, sólo se copiarán con el documento los archivos cargados y adjuntados en Biblioteca, Lista de repositorios. Los adjuntos de archivo cargados desde otras ubicaciones no se copian con el documento.

Visualización de historiales de documento

Puede revisar un registro de todas las acciones ejecutadas en un documento.

Para historiales de documento, haga clic en la ficha Historial de la página Actualizar documento.

Aparece una lista de eventos que muestra los detalles de cada evento. La información mostrada en la ficha Historial sólo existe como referencia y no se puede modificar.

Notificaciones de documentos

En CA Service Desk Manager, puede configurar una lista de usuarios, conocidos como contactos, que pueden ser notificados cuando se produzcan determinados eventos. El proceso de notificación informa a los individuos del estado de cambio de un documento, y los mantiene al día sobre su progreso. Sólo se puede enviar notificaciones designadas para el documento a los usuarios que aparecen en esta lista.

Cambios del documento

En cuanto algún documento llega a una carpeta de bandeja de entrada en el panel de resultados, los usuarios pueden realizar las tareas asignadas al modificar y guardar los documentos de acuerdo con los roles que se les ha asignado; por ejemplo, un analista puede ser responsable de comprobar el contenido técnico de los documentos mientras que otro se ocupa del formato.

Cualquier usuario que disponga de todos los permisos para un determinado documento puede modificarlo. El propietario actual dispone de todos los permisos del documento, aunque no se explicita el permiso de escritura. Sólo el propietario tiene capacidad para cambiar el propietario de los documentos (en la ficha Atributos).

Cómo gestionar los privilegios de rol y la visibilidad del documento

Puede configurar los permisos de seguridad de Gestión del conocimiento gestionando los privilegios de rol para los usuarios de su entorno. Con estos permisos es posible determinar qué usuarios pueden acceder cuando desean ver o crear conocimiento, y cómo se autentican al iniciar sesión en el sistema.

Para gestionar los privilegios de rol y la visibilidad del documento para Gestión del conocimiento, realice lo siguiente:

1. En la ficha Administración, seleccione Gestión de seguridad y de roles, Gestión de roles, Lista de roles.
Aparecerá la página Lista de roles.
2. Seleccione el rol que desee como, por ejemplo, Gestor de conocimientos. Las páginas Detalles de rol y Actualizar rol muestran las siguientes fichas:

Gestión del conocimiento

Especifica los privilegios de Gestión del conocimiento para el rol.

Visibilidad de documento de KT

Especifica los estados de documento que el rol puede ver, como borrador, retirado y publicado.

3. Complete las páginas de ficha y guarde los cambios.

Se definen la seguridad y los privilegios de rol.

Nota: Para obtener más información sobre la configuración de seguridad y la definición de roles, consulte la *Ayuda en línea*.

Contenido de acción

Puede crear "contenido de acción" (una URL dinámica) que se puede insertar en el campo Resolución de un documento de conocimiento que, cuando el usuario final hace clic en él, crea un incidente o realiza alguna otra acción. Al usar contenido de acción, se puede lograr un grado considerable de definición y clasificación sin que el usuario se dé cuenta.

Los pasos para insertar un vínculo dinámico de "contenido de acción" en un documento son sencillos y no se requiere codificación. El editor HTML de Gestión del conocimiento trata la generación del código HTML.

Nota: El contenido de acción se utiliza principalmente para la interacción con aplicaciones externas.

Más información:

[Visualización de contenido de acción](#) (en la página 831)

[Creación de contenido de acción \(URL de la acción\)](#) (en la página 832)

[Creación de contenido de acción \(HTML interno\)](#) (en la página 833)

[Edición de contenido de acción](#) (en la página 833)

[Búsqueda de contenido de acción](#) (en la página 834)

Visualización de contenido de acción

Puede ver los detalles de las URL de acción dinámica que permiten definir acciones para los usuarios finales. Gestión del conocimiento permite vincular documentos de conocimiento con tareas automatizadas, para que pueda incrustar scripts de autoservicio en los documentos de conocimiento.

Procedimiento para ver contenido de acción

1. En la ficha Administración, vaya a Conocimiento, Contenido de acción.
Aparecerá la Lista de contenidos de acción.
2. La página muestra detalles de acción y opciones de ejecución.

Nombre

Muestra el nombre del contenido de acción.

Código

Especifica el código HTML que vincula el contenido de acción con el documento.

URL de la acción

Especifica el vínculo de URL que realiza algún tipo de acción, como abrir un sitio Web o un formulario.

Búsqueda

Busca elementos por nombre.

Mostrar filtro

Busca elementos en la página Lista de comentarios. Puede rellenar uno o varios campos de búsqueda y hacer clic en Buscar. La página Lista de contenidos de acción muestra los elementos que coinciden con los criterios seleccionados.

Crear nuevo

Crea un vínculo de contenido de acción.

3. Busque contenido de acción que pueda utilizar con Gestión del conocimiento y Automatización de soporte.
Aparecerán los resultados de la búsqueda.

Creación de contenido de acción (URL de la acción)

Puede crear contenido de acción para documentos de conocimiento. Estas URL de acción pueden iniciar un sitio Web dinámico que sea accesible para todos los usuarios del sistema. También es posible conectar las URL de acción con tareas automatizadas en el servidor, así como incrustar estos scripts en documentos de conocimiento, documentos de árbol, plantillas de documento y foros de conocimiento.

Procedimiento para crear contenido de acción (URL de la acción)

1. En la ficha Administración, vaya a Conocimiento, Contenido de acción.
Aparecerá la página Lista de contenidos de acción.
2. Haga clic en Crear nuevo.
Se muestra la página Crear nuevo contenido de la acción.
3. Rellene los campos. The following fields require explanation:

Código

Especifica un identificador exclusivo para este elemento de contenido de acción.

Utilizar HTMPL interno

Crea un vínculo interno (see page 833) en la aplicación que transmite dinámicamente información, como el nombre de usuario e ID de sesión, desde los documentos de conocimiento a las aplicaciones de terceros. No seleccione esta opción.

URL de la acción

Especifica una URL que vincula a una página Web, plantilla o script automatizado, por ejemplo: <http://www.ca.com>.

Haga clic en Guardar.

Se creará el contenido de acción.

Creación de contenido de acción (HTMPL interno)

Puede crear contenido de acción para documentos de conocimiento. Estas URL de acción pueden iniciar scripts de autoservicio y también aplicaciones de terceros. Este vínculo se genera dinámicamente y transfiere de forma automática atributos sobre el usuario, como el nombre de usuario, a la aplicación de destino (<http://www.ca.com?USERNAME=BBB>, por ejemplo). Los atributos de usuario se especifican en un archivo HTMPL.

Procedimiento para crear contenido de acción con un archivo HTMPL interno

1. Cree un archivo HTMPL interno que transmita datos a la aplicación de destino.

Nota: El archivo `act_content_sample.html` está disponible en la siguiente ubicación: `NX_ROOT\bopcfg\www\html\default`.

2. Guarde el archivo HTMPL en la siguiente ubicación: directorio `NX_ROOT\site\mods\www\html\default`.
3. En la ficha Administración, vaya a Conocimiento, Contenido de acción. Aparecerá la página Lista de contenidos de acción.
4. Haga clic en Crear nuevo. Aparecerá la página Crear nuevo contenido de la acción.
5. Rellene el siguiente campo:

Código

Especifica un identificador exclusivo para este elemento de contenido de acción.

6. Active la casilla de verificación Utilizar HTMPL interno.
7. Especifique el archivo HTMPL apropiado en el campo URL de la acción, por ejemplo: `act_content_sample.html`

Nota: Puede utilizar scripts de Automatización de soporte con el formato `SA_SCRIPT=[Self Service Script ID]` en la URL.

8. Haga clic en Guardar.

Se creará el contenido de acción. Cuando el usuario hace clic en este vínculo de contenido de acción en un documento de conocimiento, los atributos sobre el usuario, como el nombre de usuario, se transmiten dinámicamente a la aplicación de destino.

Edición de contenido de acción

Puede editar el contenido de acción que ya se ha creado en la página Lista de contenidos de acción.

Procedimiento para editar contenido de acción

1. En la ficha Administración, seleccione Conocimiento, Contenido de acción.
Aparecerá la Lista de contenidos de acción.
2. Seleccione el elemento que desea editar.
Aparecerá la página Detalles de contenido de la acción.
3. Haga clic en Editar.
Aparecerá la página Actualizar contenido de acción.
4. Edite en los campos según sea necesario.
5. Haga clic en Guardar.
Se actualizará el contenido de acción.

Búsqueda de contenido de acción

Puede introducir criterios de búsqueda para filtrar la lista de contenidos de acción para que sólo se muestren los elementos que desea ver. También puede buscar elementos individuales que desee ver o editar.

Procedimiento para buscar contenido de acción

1. En la ficha Administración, seleccione Conocimiento, Contenido de acción.
Se abre la página Lista de contenidos de acción.
2. Haga clic en Mostrar filtro.
Aparecerá el filtro de búsqueda.
3. Rellene uno o varios campos de búsqueda:

Nombre

Identifica el elemento del contenido de acción.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Indica si el elemento está activo o inactivo.

Código

Especifica un identificador exclusivo para este elemento de contenido de acción.

URL de Gestión del conocimiento

Especifica que la URL de acción se vincula a la página Web interna (.html).

4. (Opcional) Haga clic en Más.

Se muestran más campos que permiten restringir aún más los elementos que aparecen en la Lista de contenidos de la acción.

5. Haga clic en Buscar.

La página Lista de contenidos de la acción muestra los elementos que coinciden con los criterios de búsqueda. Puede seleccionar un elemento para verlo o editarlo.

Nota: Puede exportar los resultados de la lista a Excel para su uso fuera de CA Service Desk Manager haciendo clic en el botón Exportar en la página de lista.

Proceso de aprobación del documento

Para los administradores que desean controlar la gestión de la base de conocimiento, la capacidad de personalizar la edición de documentos y el proceso de aprobación son esenciales. Puede diseñar plantillas de proceso de aprobación que especifican cómo, cuándo y a través de cuál plantilla se puede modificar y publicar un documento de empleado. Las plantillas de proceso de aprobación pueden designar diferentes procesos de aprobación que se ajusten mejor al entorno de negocios. El proceso de aprobación que se implementa se puede modificar gradualmente para hacerlo más sencillo o más complejo.

El gestor del proceso de aprobación permite definir plantillas de proceso de aprobación. De forma predeterminada, se utiliza la plantilla de proceso de aprobación integrada. Sin embargo, se puede crear una plantilla o editar una existente. Al crear una plantilla de proceso de aprobación, se deben definir los estados y agregar tareas a la plantilla. El proceso de aprobación involucra una serie de tareas que se realizan en un documento de conocimiento. El propietario que está asignado a la tarea en la plantilla de proceso de aprobación ejecuta cada tarea.

A continuación se presentan los diferentes estados con los que está asociado el documento durante las fases del proceso de aprobación:

Borrador

Especifica un nuevo documento.

Publicado

Especifica un documento que ha pasado a través del ciclo de aprobación completo y pasa a formar parte de la base de conocimiento visible.

Versión del Rework-Draft

Especifica una versión modificada de una copia del documento que se sustituye en la base de conocimiento después de verificarlo y volverlo a publicar.

Retirado

Especifica un documento que ha alcanzado su fecha de caducidad. También se pueden crear estados personalizados, para asociar posteriormente con las tareas.

Gestor de procesos de aprobación

Los administradores de conocimiento pueden utilizar al gestor del proceso de aprobación para realizar estas acciones:

- Determinar qué grupos pueden leer un documento de conocimiento y qué grupos pueden escribir (o editar) un documento de conocimiento.
- Identificar las tareas en una plantilla de proceso de aprobación que determinan el ciclo de vida de los documentos creados con la plantilla.
- Definir los diversos estados a los que se puede asociar el documento durante el proceso de aprobación.

Importante: al crear un documento de conocimiento, verifique que los permisos del documento incluyan usuarios que pueden asignarse más tarde al documento mediante el proceso de aprobación. Los usuarios de ese grupo no necesariamente tienen permiso para ver el documento. Si el documento está asignado a un usuario específico, las restricciones de partición de datos predeterminadas permiten al usuario ver el documento.

Definición de un proceso de aprobación para la edición de documentos

Los administradores de conocimiento pueden especificar quién puede editar documentos antes del proceso de aprobación y después de la publicación.

Nota: Los usuarios con todos los permisos (de lectura y escritura) pueden editar documentos publicados.

Procedimiento para definir un proceso de aprobación para la edición de documentos

1. En la ficha Administración, vaya a Conocimiento, Gestor del proceso de aprobación, Valores de proceso de aprobación.

Aparecerá la página Valores de proceso de aprobación.

2. Especifique quién puede editar documentos *antes* de su publicación. Seleccione una de las siguientes opciones:

Los documentos los deben editar un asignatario de tareas, un propietario o usuarios con las vistas de tipo de acceso adecuadas.

Especifica que los siguientes contactos pueden editar documentos:

- Un contacto asignado a la tarea actual
- Un contacto especificado como propietario del documento con respecto a la tarea actual
- Un gestor de conocimientos
- Un administrador del sistema

Los documentos los deben editar usuarios con todos los permisos.

Especifica que cualquier usuario con permisos de escritura en el documento puede editarlo.

3. Especifique quién puede editar documentos *después* de su publicación. Seleccione una de las siguientes opciones:

Un usuario con todos los permisos puede editar un documento una vez publicado.

Especifica que un usuario con todos los permisos puede editar documentos publicados.

Un usuario con todos los permisos puede cambiar los atributos del documento publicado

Especifica que cualquier usuario con permisos de escritura en el documento puede cambiar solamente los atributos de los documentos publicados como elementos de configuración o productos.

Se debe anular la publicación del documento antes de permitir la edición

Especifica que el usuario debe anular la publicación de un documento antes de editarlo.

Haga clic en Guardar.

Se define el proceso de aprobación.

Creación de plantillas de proceso de aprobación

Las tareas de una plantilla de proceso de aprobación definen el ciclo de vida de los documentos creados con la plantilla.

Nota: Si el multicliente está instalado, seleccione el cliente apropiado de la lista desplegable. La opción público (compartida) crea el objeto para todos los clientes.

Procedimiento para crear una plantilla de proceso de aprobación

1. En la ficha Administración, seleccione Conocimiento, Gestor del proceso de aprobación, Plantillas de procesos de aprobación.

Aparecerá la Lista de plantillas de proceso de aprobación.

2. Haga clic en Crear nuevo.

Aparecerá la página Detalles de la plantilla del proceso de aprobación.

3. Escriba un nombre para la plantilla y una descripción.

4. Haga clic en Guardar.

La página Detalles de la plantilla del proceso de aprobación muestra campos complementarios.

5. Seleccione la tarea que desea realizar al crear una versión modificada del documento mediante esta plantilla.

6. Seleccione la tarea que desea realizar cuando anule la retirada de un documento creado mediante esta plantilla.

7. Haga clic en Insertar tarea para crear una tarea para agregarla a la plantilla.

Aparecerá la página Crear nueva tarea.

8. Rellene los campos. The following fields require explanation:

Tarea

Asigna un nombre a la tarea.

Asignado

Asigna la tarea a una persona. Puede hacer clic en el icono de búsqueda para seleccionar un nombre.

Nota: Puede agregar una lista alternativa de asignatarios (see page 839) después de que se crea la tarea.

Haga clic en Guardar.

Se crea la plantilla de proceso de aprobación.

Más información:

[Cómo agregar asignatarios alternativos a una tarea](#) (en la página 839)

[Cómo editar una plantilla de proceso de aprobación](#) (en la página 839)

[Búsqueda de plantillas de proceso de aprobación](#) (en la página 840)

Cómo agregar asignatarios alternativos a una tarea

Puede agregar asignatarios alternativos al editar una tarea.

Procedimiento para agregar asignatarios alternativos a una tarea

1. Seleccione la tarea que desea editar en la Lista de plantillas de proceso de aprobación.
Aparecerá la página Detalles de tarea.
2. Edite los campos según sea necesario.
3. Haga clic en el botón Agregar en la Lista de asignatarios.
Aparecerá la página Crear nuevo asignatario.
4. En el campo Asignatario, escriba el nombre de la persona a la que desea asignar la tarea, o bien haga clic en el icono de búsqueda para seleccionar el nombre.
5. Repita el paso 4 según sea necesario para crear una lista de asignatarios alternativos.
6. Haga clic en Guardar.
Los asignatarios alternativos se agregan a la tarea.

Cómo editar una plantilla de proceso de aprobación

Puede editar una plantilla de proceso de aprobación.

Procedimiento para editar una plantilla del proceso de aprobación

1. En la ficha Administración, seleccione Conocimiento, Gestor del proceso de aprobación, Plantillas de procesos de aprobación.
Aparecerá la Lista de plantillas de proceso de aprobación.

2. Seleccione la plantilla que desee editar y haga clic en su nombre.
Aparecerá la página Detalles de la plantilla del proceso de aprobación.
3. Haga clic en Editar.
Aparecerá la página Actualizar plantilla de proceso de aprobación.
4. Edite los campos según sea necesario.
5. Haga clic en Guardar.
Se actualiza la plantilla de proceso de aprobación.

Búsqueda de plantillas de proceso de aprobación

Puede introducir criterios de búsqueda para filtrar la Lista de plantillas de proceso de aprobación para que sólo se muestren los elementos que desea ver. También puede buscar elementos individuales que desee ver o editar.

Nota: Si multicliente está instalado, la página de lista muestra la configuración de datos públicos y de clientes en el filtro de búsqueda. Los datos públicos se pueden excluir o incluir con los datos de clientes; sólo se buscan objetos públicos exclusivamente. En las páginas de detalles, seleccione el cliente apropiado de la lista. Si selecciona <vacío>, el objeto es público.

Procedimiento para editar una plantilla de proceso de aprobación

1. En la ficha Administración, seleccione Conocimiento, Gestor del proceso de aprobación, Plantillas de procesos de aprobación.
Aparecerá la página Lista de plantillas de proceso de aprobación.
2. Haga clic en Mostrar filtro.
3. Escriba los primeros caracteres del nombre de la plantilla que desee.
4. (Opcional) Haga clic en Más.
Se muestran más campos que permiten restringir aún más los elementos que aparecen en la Lista de plantillas de proceso de aprobación.
5. Haga clic en Buscar.
La página Lista de plantillas de proceso de aprobación muestra los elementos que coinciden con los criterios de búsqueda introducidos. Puede seleccionar un elemento para verlo o editarlo.

Nota: Puede exportar los resultados de la lista a Excel para su uso fuera de CA Service Desk Manager haciendo clic en el botón Exportar en la página de lista.

Definiciones de estado del documento

Puede agregar y suprimir estados de documento definidos por el usuario, así como modificar los nombres y las descripciones de los estados de documento predefinidos.

Más información:

[Creación de estados de documento](#) (en la página 841)

[Búsqueda de estados de documento](#) (en la página 841)

[Edición del estado de documento](#) (en la página 842)

Creación de estados de documento

Puede crear un estado de documento para documentos de conocimiento en el sistema de CA Service Desk Manager.

Procedimiento para crear un estado de documento

1. En la ficha Administración, seleccione Conocimiento, Gestor del proceso de aprobación, Estados del documento.
Aparecerá la Lista de estados de documento.
2. Haga clic en Crear nuevo.
Aparecerá la página Detalles de estado de documento.
3. Escriba un nombre para el estado y una descripción.
4. Haga clic en Guardar.
Se crea el estado del documento.

Búsqueda de estados de documento

Puede introducir criterios de búsqueda para filtrar la lista de estados de documento para que sólo se muestren los elementos que desea ver. También puede buscar elementos individuales que desee ver o editar.

Procedimiento para buscar un estado de documento

1. En la ficha Administración, seleccione Conocimiento, Gestor del proceso de aprobación, Estados del documento.
Aparecerá la página Lista de estados de documento.
2. Haga clic en Mostrar filtro.
3. Escriba los primeros caracteres del nombre de estado que desee buscar.
4. (Opcional) Haga clic en Más.
Se muestran más campos que permiten restringir los elementos que aparecen en la Lista de estados de documento.

5. Haga clic en Buscar.

La página Lista de estados de documento muestra los elementos que coinciden con los criterios de búsqueda. Puede seleccionar un elemento para verlo o editarlo.

Nota: Puede exportar los resultados de la lista a Excel para su uso fuera de CA Service Desk Manager haciendo clic en el botón Exportar en la página de lista.

Edición del estado de documento

Puede editar el estado de un documento.

Procedimiento para editar el estado de un documento

1. En la ficha Administración, seleccione Conocimiento, Gestor del proceso de aprobación, Estados del documento.
Aparecerá la Lista de estados de documento.
2. Seleccione el estado que desee editar y haga clic en su nombre.
Aparecerá la página Detalles de estado de documento.
3. Haga clic en Editar.
Aparecerá la página Actualizar estado de documento.
4. Edite el estado y los campos de descripción según corresponda.
5. Haga clic en Guardar.
Se actualiza el estado del documento.

Políticas automatizadas

Los administradores pueden automatizar ciertas tareas en el proceso de aprobación del documento de conocimiento según las acciones y las políticas de ciclo de vida de los documentos que definan. Al automatizar tareas, los usuarios finales que están buscando soluciones pueden resolver problemas más rápidamente y pueden hacerlo sin ponerse en contacto con otros individuos, lo cual proporciona un beneficio a la organización.

Las políticas automatizadas funcionan con la opción Eventos y macros.

Más información:

[Visualización de políticas automatizadas](#) (en la página 843)

[Cómo configurar políticas automatizadas](#) (en la página 844)

[Creación de una política automatizada](#) (en la página 845)

[Edición de una política automatizada](#) (en la página 846)

[Programación de políticas automatizadas](#) (en la página 846)

[Visualización de informes de políticas de ciclo de vida de los documentos](#) (en la página 847)

Visualización de políticas automatizadas

Las políticas automatizadas describen la condición por la que se marcan los documentos para la corrección y por la que se promueven para su publicación o retiro durante las distintas fases del proceso del ciclo de vida de los documentos. Por ejemplo, se puede especificar la política predeterminada "corregir vínculos rotos" que coincide con los documentos encontrados en la base de conocimiento con vínculos rotos. La tarea de corregir el problema se le puede asignar a un analista.

Nota: Si multicliente está instalado, la página de lista muestra la configuración de datos públicos y de clientes en el filtro de búsqueda. Los datos públicos se pueden excluir o incluir con los datos de clientes; sólo se buscan objetos públicos exclusivamente. En las páginas de detalles, seleccione el cliente apropiado de la lista. Si selecciona <vacío>, el objeto es público.

Para ver políticas automatizadas, seleccione la ficha Administración, Conocimiento, Políticas automatizadas, Políticas.

La página Lista de políticas automatizadas muestra los detalles de las políticas automatizadas. Puede editar las políticas predeterminadas o definir unas propias. Cada política se asocia con los siguientes componentes:

Consulta almacenada

Contiene un conjunto de macros de acción que se ejecutan cuando las políticas identifican un documento y coinciden con él durante el procesamiento. Tras el procesamiento, el evento de condición de consulta almacenada muestra un informe de política de ciclo de vida de Gestión del conocimiento basado en roles en el panel de resultados de CA Service Desk Manager.

El administrador es responsable de controlar los informes y proporcionar evaluación y recomendaciones a los editores de documentos apropiados.

Macro de acción

Contiene código que permite a los usuarios establecer un indicador, aumentar la prioridad o realizar alguna otra acción. Puede modificar las macros que aparecen en la lista de macros o definir unas propias.

Nota: Puede exportar los resultados de la lista a Excel para su uso fuera de CA Service Desk Manager haciendo clic en el botón Exportar en la página de lista.

Más información:

[Visualización de informes de políticas de ciclo de vida de los documentos](#) (en la página 847)

[Programación de políticas automatizadas](#) (en la página 846)

Cómo configurar políticas automatizadas

Los administradores pueden establecer la opción Políticas automatizadas si llevan a cabo los siguientes pasos:

1. (Obligatorio) Se debe definir un proceso por lotes en el Planificador de políticas automatizadas que se ejecuta en el servidor a fin de presentar los datos necesarios para ver los informes de política del ciclo de vida de Gestión del conocimiento. Este paso de acción también se aplica a la tarjeta de informes de conocimiento.

Nota: Para obtener más información sobre políticas automatizadas, consulte la *Guía de implementación*.

2. (Obligatorio) Para gestionar la seguridad y los roles, defina la fase en la que los usuarios pueden ver y buscar en documentos durante su ciclo de vida en la ficha Visibilidad del documento de conocimiento de Administración de roles.
3. En la página Lista de políticas automatizadas, puede editar las políticas predeterminadas o definir unas propias.

Nota: Cuando un documento está abierto para su edición, en la ficha Atributos aparece de forma predeterminada una casilla de verificación que, si se activa, descarta (u omite) todas las políticas del ciclo de vida. En el caso de las políticas nuevas, el administrador debe incluir el campo "Descartar políticas de ciclo de vida" en la consulta almacenada; de lo contrario, no aparece en la ficha Atributos.

Creación de una política automatizada

Puede crear una política automatizada que se active cuando se produzca una acción, como cuando se publica un documento o se retira de la base de conocimiento.

Nota: Si el multicliente está instalado, seleccione el cliente apropiado de la lista desplegable. La opción público (compartida) crea el objeto para todos los clientes.

Procedimiento para crear una política automatizada

1. En la ficha Administración, vaya a Conocimiento, Políticas automatizadas, Políticas.
Aparece la página Crear nueva política automatizada.
2. Introduzca un nombre y una descripción para la política en los campos correspondientes.
3. Introduzca un nombre de consulta almacenada o seleccione uno con el icono de búsqueda.
4. Haga clic en Agregar acción.
Aparecerá la página Lista de macros.
5. En la página Lista de macros, seleccione una de las macros de acción predefinidas o defina unas propias (haga clic en Crear nuevo).
La macro de acción aparece en la lista Información de acción de la página Crear nueva política automatizada.
Nota: Puede suprimir una macro de acción. Para ello, haga clic con el botón secundario en el nombre y seleccione Suprimir en el menú contextual.
6. Haga clic en Guardar.
La nueva política aparecerá en la lista de políticas automatizadas.
7. (Opcional) Haga clic en el título para editar una política.
La política seleccionada aparece en la página Actualización de políticas y puede editarla.

Edición de una política automatizada

Puede actualizar una política automatizada.

Procedimiento para editar una política automatizada

1. En la ficha Administración, vaya a Conocimiento, Políticas automatizadas, Políticas.

Aparecerá la lista de políticas automatizadas.

2. Haga clic con el botón secundario en la política que desee editar y seleccione Editar en el menú contextual.

Aparecerá la página Actualizar política automatizada

3. Edite los campos de entrada según sea necesario.
4. Haga clic en Guardar.

Se actualiza la política automatizada.

Programación de políticas automatizadas

Puede especificar la fecha y hora en que CA Service Desk Manager realiza el cálculo y ejecuta el proceso por lotes de las políticas.

Procedimiento para programar políticas automatizadas

1. Seleccione la ficha Administración, vaya a Conocimiento, Políticas automatizadas, Programación.

Aparecerá la página Políticas automatizadas.

2. Rellene los siguientes campos:

Última modificación

Especifica la casilla de verificación Ejecutar cálculo.

Programación

Especifica una fecha en el cuadro de texto o en el Calendario. Puede seleccionar el intervalo de tiempo en que CA Service Desk Manager realiza el cálculo y ejecuta las políticas.

Haga clic en Guardar.

Las políticas se procesan en la fecha y hora especificadas.

Visualización de informes de políticas de ciclo de vida de los documentos

Puede ver los informes de política del ciclo de vida de los documentos que generan las políticas automatizadas.

Para mostrar los informes, seleccione la ficha Service Desk, Documentos de conocimiento, Políticas automatizadas, Políticas.

Cuando selecciona una política, aparece la siguiente información de resumen en la página Lista de documentos:

Nota: Si multicliente está instalado, la página de lista muestra la configuración de datos públicos y de clientes en el filtro de búsqueda. Los datos públicos se pueden excluir o incluir con los datos de clientes; sólo se buscan objetos públicos exclusivamente. En las páginas de detalles, seleccione el cliente apropiado de la lista. Si selecciona <vacío>, el objeto es público.

Título

Muestra el título del documento que se marca para su corrección o se promueve para su publicación o retiro.

Política/acciones

Muestra el nombre de la política y el contenido de acción definidos para la política.

Atributos

Muestra las propiedades del documento al que afecta la política a la que éste se asigna.

Control del documento de conocimiento

Cuando el usuario abre un documento de conocimiento, puede agregar comentarios, enviar conocimiento y ver sus documentos de árbol de conocimiento. También puede especificar el contenido y el aspecto de los documentos mediante la selección de una plantilla.

Los administradores pueden controlar cómo interactúan los usuarios con los documentos mediante las siguientes tareas:

- Definir los tipos de comentarios (see page 848) que aparecen en los documentos de conocimiento y listas desplegables en la interfaz de usuario de final.
- Especificar valores (see page 911) de documento en relación con comentarios, envío de conocimiento y visualización de documentos.

- Crear plantillas de documento (see page 853) que especifiquen el contenido y el aspecto de los documentos.
- Exportar (see page 800) (o importar) contenido de conocimiento desde otro recurso o sistema.
- Gestionar características de control de versiones (see page 785) de documentos.
- Gestionar la Programación de documentos de conocimiento (see page 789).

Véase también

[Tipos de comentarios](#) (en la página 848)

[Plantillas de documento](#) (en la página 853)

[Cómo crear vínculos de documentos de conocimiento](#) (en la página 861)

Tipos de comentarios

Si los analistas encuentran una errata o un problema relacionado con el contenido de un documento, pueden agregar un comentario que marcará el documento para su corrección y, a continuación, asignar el problema a otro analista para que realice el seguimiento.

Los administradores pueden definir los tipos de comentario que aparecen en distintas vistas de listas en la interfaz de usuario final.

Visualización de tipos de comentarios

Cuando los usuarios abren un documento de conocimiento, pueden agregar un comentario que marcará el documento para su corrección, promoción o retiro, entre otras muchas tareas. La página Lista de tipos de comentarios permite gestionar los detalles de los tipos de comentarios.

Para mostrar esta página, seleccione la ficha Administración, Conocimiento, Documentos, Tipos de comentarios.

Nota: Si multicliente está instalado, la página de lista muestra la configuración de datos públicos y de clientes en el filtro de búsqueda. Los datos públicos se pueden excluir o incluir con los datos de clientes; sólo se buscan objetos públicos exclusivamente. En las páginas de detalles, seleccione el cliente apropiado de la lista. Si selecciona <vacío>, el objeto es público.

Aparecerá la página Lista de tipos de comentarios y se muestran las siguientes columnas:

Nombre

Muestra la lista de tipos de comentarios que aparecen en los documentos y listas desplegables en la interfaz de usuario. Puede editar los siguientes tipos de comentarios predeterminados o definir unos propios:

- Vínculo roto
- Candidato para publicación
- No se ha borrado el contenido
- Difícil de encontrar
- Comentario general
- Información incorrecta
- Información que falta
- Recomendar contenido nuevo
- Revisión
- La solución no funciona

Mostrar en la vista de usuario

Muestra el comentario en diversas vistas de lista en la interfaz de usuario.

Seguimiento obligatorio

Especifica si es necesario que el usuario responda a este tipo de comentario.

Tiempo para finalización (días)

Define el número de días durante los cuales el usuario debe seguir este tipo de comentario.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Indica si el tipo de comentario está activo o inactivo.

Esta página contiene los siguientes botones:

Búsqueda

Busca elementos por nombre.

Mostrar filtro

Busca un comentario en la página Lista de comentarios. Rellene uno o varios campos de búsqueda y haga clic en Buscar. La página Lista de tipos de comentarios muestra los comentarios que coinciden con los criterios introducidos.

Borrar filtro

Borra el filtro.

Crear nuevo

Crea un tipo de comentario.

Nota: Puede exportar los resultados de la lista a Excel para su uso fuera de CA Service Desk Manager haciendo clic en el botón Exportar en la página de lista.

Creación de tipos de comentario

Puede definir los tipos de comentarios que aparecen en diversas vistas de lista en la interfaz de usuario final de la página Crear nuevo tipo de comentario.

Nota: Si el multicitente está instalado, seleccione el cliente apropiado de la lista desplegable. La opción público (compartida) crea el objeto para todos los clientes.

Procedimiento para crear un tipo de comentario

1. En la ficha Administración, seleccione Conocimiento, Documentos, Tipos de comentarios.

Aparecerá la página Lista de tipos de comentarios.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nuevo tipo de comentario.

3. Rellene los campos según sea necesario. The following fields require explanation:

Tiempo para finalización (días)

Define el número de días durante los cuales el usuario debe seguir este tipo de comentario.

Mostrar en la vista de usuario

Muestra el comentario en diversas vistas de lista en la interfaz de usuario.

Seguimiento obligatorio

Especifica si es necesario que el usuario responda a este tipo de comentario.

Haga clic en Guardar.

El nuevo tipo de comentario aparece en la página Lista de tipos de comentarios.

Edición de tipos de comentario

Puede actualizar un tipo de comentario que ya se ha creado en la página Lista de tipos de comentarios.

Procedimiento para editar un tipo de comentario

1. En la Lista de tipos de comentarios, realice una de las siguientes acciones:
 - Seleccione un comentario y seleccione Editar en la página Detalles de tipo de comentario.
 - Haga clic con el botón secundario en un comentario y seleccione Editar en el menú contextual.

Aparecerá la página Detalles de tipo de comentario.

2. Rellene los campos según sea necesario.
3. Haga clic en Guardar.

El tipo de comentario actualizado aparece en la página Lista de tipos de comentarios.

Notificaciones de documentos

En CA Service Desk Manager, puede configurar una lista de usuarios, conocidos como contactos, que pueden ser notificados cuando se produzcan determinados eventos. El proceso de notificación informa a los individuos del estado de cambio de un documento, y los mantiene al día sobre su progreso. Sólo se puede enviar notificaciones designadas para el documento a los usuarios que aparecen en esta lista.

Configuración de notificaciones de comentarios de seguimiento

Varias notificaciones de actividad predeterminadas enumeradas en la página Lista de notificaciones de actividades permiten configurar notificaciones para los usuarios cuando se les asigna un comentario de seguimiento.

La cola de comentarios de seguimiento en el panel de resultados es el repositorio de comentarios de seguimiento asignados y sin asignar.

Procedimiento para configurar notificaciones de comentarios de seguimiento

1. En la ficha Administración, vaya a Notificaciones, Notificaciones de actividades.

Aparecerá la página Lista de notificaciones de actividades.

2. Seleccione *una* de las siguientes notificaciones de actividades:
 - Comentario de seguimiento asignado
 - Comentario de seguimiento cerradoAparecerá la página Detalles de notificaciones de actividades.
3. Haga clic en Editar.
Aparecerá la página Actualizar notificaciones de actividades.
4. Cambie los campos según corresponda.
5. Haga clic en Guardar.
Aparecerá la página Detalles de notificaciones de actividades.
6. Haga clic en Cerrar ventana.
La notificación de actividad modificada aparecerá en la lista de notificaciones de actividades cuando se vuelva a mostrar la lista.

Especificación de la configuración del documento

Si es administrador del sistema puede especificar valores de configuración en relación con comentarios, envío de conocimiento y visualización de documentos de árbol de conocimiento.

Procedimiento para especificar la configuración de documentos

1. En la ficha Administración, seleccione Conocimiento, Documentos, Valores de documento.
Aparecerá la página Valores de documento.
2. Rellene los siguientes campos:

Visualización del documento de árbol de conocimientos

Especifica el modo de visualización en el que se abren los documentos de árbol de conocimientos. Seleccione Abrir en modo de árbol (valor predeterminado) para abrir el árbol de conocimiento directamente o Abrir en modo de documento para abrir el documento en vista de documento. Si lo abre en modo de documento, haga clic en Mostrar para que aparezca el árbol de conocimiento.

Comentarios

Especifica si los usuarios pueden enviar y ver comentarios de documentos. Seleccione una de las siguientes opciones:

- **Permitir el envío y visualización de comentarios (valor predeterminado):** muestra un campo de comentarios en la parte inferior de un documento abierto para que los usuarios puedan enviar comentarios de documentos. Los usuarios pueden ver comentarios ya asociados al documento abierto.

- **Permitir el envío pero no la visualización de comentarios:** muestra un campo de comentarios a la derecha de un documento abierto para que los usuarios puedan enviar comentarios de documentos. Los usuarios no pueden ver comentarios ya asociados al documento abierto.
- **No permitir ni el envío ni la visualización de comentarios:** impide que los usuarios puedan enviar o ver comentarios. El campo de comentarios no se muestra en un documento abierto.

Enviar conocimientos

Define el repositorio para documentos enviados por el usuario. El producto rellena la lista con los nombres de los repositorios definidos en el panel Biblioteca de adjuntos.

Tamaño máximo de resolución

Define el tamaño máximo (en caracteres) que puede tener el campo Resolución de un documento.

Límites: el número máximo de caracteres permitido es 256000.

Predeterminado: 32768

Evasión de documentos duplicados

Fuerza una búsqueda de documentos similares cuando el usuario crea un documento de conocimiento.

Notificación antes de caducar

Define el número de días que transcurre antes de que caduque el documento y se envíe una notificación.

Valor predeterminado: 7

Nota: Este valor sólo se aplica a los documentos que se han actualizado o creado en CA Service Desk Manager. Si se migran documentos de CA Service Desk Manager r11.2 y las fechas de caducidad se establecen antes de la migración, esta opción no se aplicará, hasta que se actualice el documento después de la migración.

Haga clic en Guardar.

Los cambios se aplican cuando se abre un documento de conocimiento o un documento de árbol de conocimiento.

Plantillas de documento

Puede utilizar plantillas de documento para controlar el formato y el contenido predeterminado de los documentos de conocimiento. Cada documento de conocimiento utiliza una plantilla de documento para definir sus propiedades y apariencia cuando está abierto. De forma predeterminada, una plantilla integrada se asocia con nuevos documentos de conocimiento.

El editor de plantillas le permite hacer lo siguiente:

- Diseñar una plantilla de documento que más tarde se puede asociar con un documento en la ficha Contenidos de la página Editor de documentos.
- Modificar la plantilla integrada y otras plantillas.

Mediante la edición de plantillas, puede crear plantillas que se asociarán con documentos. Con el editor HTML, puede seleccionar las opciones de Propiedades y editar las secciones Encabezado y Cuerpo.

- Actualizar las plantillas de documento a partir de una versión anterior para que se admitan relaciones de conocimiento (see page 860) como, por ejemplo, los vínculos principal-secundario.

Creación de plantillas de documento

Una plantilla de documento especifica el contenido y el aspecto de documentos en la base de conocimiento. Puede aplicar las plantillas predeterminadas:

- Documento de conocimiento integrado
- Árbol de conocimiento integrado
- Edición rápida integrada

El producto utiliza las plantillas predeterminadas cuando se crean documentos de conocimiento y documentos de árbol de conocimientos, a menos que se creen plantillas de documentos y se asocien con los documentos.

Nota: Mientras crea un documento de conocimiento, seleccione el cliente apropiado en la lista desplegable. La opción público (compartida) crea el objeto para todos los clientes.

Procedimiento para crear una plantilla de documento

1. En la ficha Administración, vaya a Conocimiento, Documentos, Plantillas de documento.

Aparecerá la página Lista de plantillas de documento.

2. Haga clic en Crear nuevo.

Aparece la página Crear nueva plantilla de documento.

3. Rellene los siguientes campos:

Plantilla

(Obligatorio) Define un nombre exclusivo para la plantilla.

Detalles

Muestra el contenido estático que aparece en documentos creados utilizando la plantilla actual. Si selecciona la opción Código fuente HTML, puede editar el código HTML del cuerpo directamente en el campo Cuerpo. Si selecciona la opción Vista rápida, el campo Cuerpo es de sólo lectura y en él se muestra el contenido estático del cuerpo tal y como se mostrará en tiempo de ejecución.

4. (Opcional) Haga clic en Establecer valores predeterminados.

Aparece la página Plantilla de valores predeterminada.

Puede establecer valores predeterminados al crear un documento. Si cambia la plantilla en un documento existente, no se produce ningún impacto.

5. (Opcional) Oculte el título, el resumen, el problema o la resolución para que no aparezcan en la plantilla.

Puede ocultar estos campos cuando desea un documento sencillo, como una plantilla de preguntas y respuestas.

6. Haga clic en Editar detalles.

Aparece la página Editor HTML y puede especificar el contenido estático y diseño de los documentos que utilizan la plantilla. Puede editar el código mediante la barra de herramientas para insertar etiquetas de marcador de posición.

Importante: puede eliminar relaciones de conocimiento, como principal, secundaria y los vínculos relacionados, si suprime las etiquetas {TAG_PARENT} y {TAG_RELATED} de la plantilla.

7. Haga clic en OK.

El campo Detalles muestra el contenido actualizado.

8. (Opcional) Haga clic en Vista rápida.

Muestra el contenido tal y como aparece en los documentos a partir de la plantilla.

9. (Opcional) Haga clic en Vista HTML.

Muestra el contenido como código HTML.

10. Haga clic en Guardar.

Aparecerá la página Detalles de plantilla de documento.

11. Haga clic en Cerrar ventana.

Los documentos nuevos que utilizan la plantilla muestran el nuevo contenido y diseño.

El nombre de la plantilla aparece en la Lista de plantillas cuando vuelve a mostrar la lista.

Nota: Los cambios en el documento que utiliza la plantilla se muestran tras iniciar una nueva sesión en el sistema.

Edición de plantillas de documento

Puede editar el nombre, diseño y contenido de una plantilla mediante Gestión del conocimiento.

Procedimiento para actualizar una plantilla de documento

1. En la ficha Administración, vaya a Conocimiento, Documentos, Plantillas de documento.

Aparecerá el panel Lista de plantillas de documento.

2. Seleccione un nombre de plantilla.

Aparecerá la página Actualizar plantilla de documento.

3. Haga clic en Editar detalles.

Se abre el editor HTML.

4. Cambie el nombre, contenido o diseño de la plantilla. Puede cambiar los siguientes campos:

Plantilla

Define un nombre exclusivo para la plantilla. Este campo es obligatorio.

Detalles

Muestra el contenido estático que aparece en documentos creados utilizando la plantilla actual. Si selecciona la opción Código fuente HTML, puede editar el código HTML del cuerpo directamente en el campo Cuerpo. Si selecciona la opción Vista rápida, el campo Cuerpo es de sólo lectura y en él se muestra el contenido estático del cuerpo tal y como se mostrará en tiempo de ejecución.

5. Haga clic en Editar detalles para especificar el contenido estático y diseño de los documentos que utilizan la plantilla.

Se abre la ventana Editor HTML.

6. Edite el código mediante la barra de herramientas para insertar etiquetas de marcador de posición. Haga clic en OK.
El campo Detalles muestra el contenido actualizado.
7. (Opcional) Haga clic en Vista rápida.
El contenido aparece como documento a partir de la plantilla.
8. (Opcional) Haga clic en Vista HTML.
El contenido aparece como código HTML.
9. Haga clic en Guardar.
Aparecerá la página Detalles de plantilla de documento.
10. Haga clic en Cerrar ventana.
Los documentos nuevos que utilizan la plantilla muestran el nuevo contenido y diseño.
Cuando se actualiza la lista, aparece en ésta un cambio en el nombre de la plantilla.

Lista de plantillas de documento

La página Lista de plantillas de documentos le permite crear y gestionar plantillas de documentos que especifican el contenido y aspecto de los documentos de la base de conocimiento.

Las siguientes plantillas predeterminadas se instalan con el producto:

- Documento de conocimiento integrado
- Árbol de conocimiento integrado
- Edición rápida integrada

El producto utiliza las plantillas predeterminadas cuando se crean documentos de conocimiento y documentos de árbol de conocimientos, a menos que se creen plantillas de documentos y se asocien con los documentos.

Nota: Si multicitiente está instalado, la página de lista muestra la configuración de datos públicos y de clientes en el filtro de búsqueda. Los datos públicos se pueden excluir o incluir con los datos de clientes; sólo se buscan objetos públicos exclusivamente. En las páginas de detalles, seleccione el cliente apropiado de la lista. Si selecciona <vacío>, el objeto es público.

Para enumerar plantillas de documento, seleccione Administración, Conocimiento, Documentos y Plantillas de documento en la ficha Administración.

Aparecerá la página Lista de plantillas de documento y se incluyen las siguientes columnas:

Nombre de plantilla

Muestra una lista de las plantillas de documento que están actualmente definidas en el producto. Seleccione un nombre de plantilla para abrir la ventana Actualizar plantilla de documento. Haga clic con el botón derecho en el nombre de una plantilla para abrir el menú contextual Nombre de plantilla, que contiene comandos para trabajar con la plantilla seleccionada.

Predeterminado

Muestra una marca para indicar que se utiliza una plantilla de forma predeterminada con los documentos nuevos o que se ha eliminado la plantilla especificada de un documento. Para establecer una plantilla como predeterminada, haga clic con el botón secundario en el nombre de la plantilla y seleccione Establecer como predeterminado en el menú contextual.

Nota: Cuando cree un documento o elimine una plantilla asociada a un documento, el producto asocia la plantilla predeterminada a éste (a menos que especifique otra plantilla en la ficha Atributos de la ventana Crear nuevo documento o de la ventana Actualizar documento de conocimiento).

Esta página contiene los siguientes campos:

Plantilla

Define el nombre de la plantilla que se utilizará en las búsquedas. Este campo sólo se muestra al hacer clic en Mostrar filtro.

Argumentos de búsqueda adicionales

Define otros criterios para incluirlos en la búsqueda. Este campo sólo se muestra cuando se hace clic en el vínculo Más del panel Búsqueda de conocimientos.

Esta página contiene los siguientes botones:

Borrar filtro

Restablece el valor predeterminado de cada campo de filtro del panel o ventana.

Crear nuevo

Abre la ventana Crear nueva plantilla de documento que permite definir una nueva plantilla de documento.

Búsqueda

Inicia una búsqueda de elementos que cumplan los criterios especificados. Si no especifica ningún criterio, el producto devuelve todos los elementos adecuados (por ejemplo, carpetas/documentos, contactos, plantillas, palabras irrelevantes o grupos de permisos).

Mostrar filtro/Ocultar filtro

Muestra u oculta campos con los que puede filtrar una búsqueda de elementos en la ventana, panel o cuadro de diálogo actual.

Nota: Puede exportar los resultados de la lista a Excel para su uso fuera de CA Service Desk Manager haciendo clic en el botón Exportar en la página de lista.

Filtrado de la lista de plantillas de documento.

Se utilizan las plantillas predeterminadas al crear documentos de conocimiento y documentos de árbol de conocimientos, a menos que se creen plantillas de documentos y se asocien con los documentos. La página Lista de plantillas de documentos le permite crear y gestionar plantillas de documentos que especifican el contenido y aspecto de los documentos de la base de conocimiento. Puede filtrar plantillas en esta página.

Procedimiento para filtrar la lista de plantillas de documento

1. Haga clic en la ficha Administración.
Aparecerá la página Administración.
2. Haga clic en Conocimiento, Documentos, Plantillas de documento.
Aparecerá la Lista de plantillas de documento.
3. Realice *alguna* de las siguientes acciones:
 - Seleccione una plantilla de la columna Nombre de plantilla.
Se abre la plantilla.
 - Busque una plantilla mediante la función de búsqueda.
Aparecerán los resultados de la búsqueda de plantillas.
 - Seleccione Mostrar filtro para filtrar la búsqueda.
Se filtra la búsqueda de plantillas.

Actualizar las plantillas de documentos para mostrar vínculos de relación de conocimiento

Puede actualizar las plantillas de documentos de conocimiento desde una versión anterior de CA Service Desk Manager para mostrar las relaciones de conocimiento. La plantilla se modifica agregando las etiquetas {TAG_PARENT} y {TAG_RELATED}, lo que permite que en los documentos que utilizan la plantilla se muestren las relaciones de documentos, como por ejemplo los vínculos principal-secundario y de cliente.

Procedimiento para modificar las plantillas para mostrar las relaciones de conocimiento

1. Abra la plantilla del documento de conocimiento.
Aparecerá la página Actualizar plantilla de documento.
2. Haga clic en Editar.
3. Seleccione la vista de código fuente HTML.
Nota: También puede hacer clic en Editar detalles, abrir el editor HTML y agregar las etiquetas {TAG_PARENT} y {TAG_RELATED}.
4. Seleccione *Seleccionar marcadores de posición de plantillas* en la lista desplegable Editar detalles para agregar las etiquetas a la plantilla del documento.
Las etiquetas se agregan a la plantilla.
5. Guarde y cierre la plantilla.
La plantilla se actualiza para mostrar relaciones de conocimiento.

Cómo crear vínculos de documentos de conocimiento

El entorno de Gestión del conocimiento se puede mantener mediante la creación de vínculos de documentos. Las relaciones de conocimiento permiten crear jerarquías de documentos y gestionar cambios para los documentos de conocimiento.

Las relaciones de conocimiento se pueden crear de la siguiente manera:

1. Definir plantillas de documento de conocimiento para mostrar u ocultar las relaciones principal-secundario en el modo de vista.

2. Crear o modificar un documento de conocimiento.

Nota: De forma predeterminada, sólo puede agregar vínculos a un documento de conocimiento no publicado. Si el documento ya está publicado, ábralo en modo de edición o reproceso para crear vínculos de documentos. Puede modificar los permisos para los documentos antes del proceso de aprobación y después de la publicación.

3. Cree *cualquiera* de los vínculos de documentos siguientes en la ficha Conocimiento relacionado, de la manera que resulte más adecuada para el entorno de Gestión del conocimiento:

- Vincular el documento como un Ver también no jerárquico.

Puede vincular documentos de conocimiento a otros documentos existentes.

- Vincular el documento como principal o secundario.

Puede conectar documentos de conocimiento en relaciones principal-secundario.

Nota: Si modifica un documento principal, aparece una que indica que se pueden los documentos secundarios pueden verse afectados.

- Vincular el documento global a un documento de cliente.

Puede vincular los documentos de conocimiento a un solo cliente o a varios clientes. Por ejemplo, un documento secundario puede tener un cliente diferente que el documento principal.

La ficha Historial se actualiza al crear los vínculos de documentos como ayuda para el seguimiento de los cambios.

4. Guarde el documento y verifique que aparezcan los vínculos al abrir el documento en la vista de usuario.

Puede verificar la aparición de los vínculos de documentos en función de los permisos que haya establecido.

Creación de un vínculo principal-secundario

Puede crear relaciones principal-secundario para los documentos de conocimiento. Los vínculos principal-secundario se utilizan para organizar documentos relacionados para los usuarios en el entorno.

Procedimiento para crear un vínculo principal-secundario

1. Cree un documento de conocimiento o abra un documento en el modo de edición.

Aparecerá el documento de conocimiento.

2. Seleccione la ficha Conocimiento relacionado.

Aparecerá la página Categorías.

Nota: Puede crear también vínculos desde la ficha Buscar similar. Utilice criterios de búsqueda para encontrar los documentos.

3. Localice el documento que quiera vincular en el panel Categorías (X).

Haga clic con el botón secundario en el documento en el panel Documentos y seleccione la opción *Vincular este documento como principal* o *Vincular este documento como Secundario* para crear el vínculo entre los documentos.

Se crea el vínculo del documento.

Creación de un vínculo Ver también

Puede crear una relación Ver también para los documentos de conocimiento del entorno. Las relaciones Ver también se utilizan para gestionar jerarquías de conocimiento en el entorno.

Procedimiento para crear un vínculo Ver también

1. Cree un documento de conocimiento o abra un documento en el modo de reproceso.

Aparecerá el documento de conocimiento.

2. Seleccione la ficha Conocimiento relacionado.

Aparecerá la página Categorías.

Nota: Puede crear también vínculos desde la ficha Buscar similar.

3. Localice el documento que quiera vincular en el panel Categorías (X).

Haga clic con el botón secundario en el panel Documentos y seleccione la opción *Vincular este documento como Ver también*.

Se crea el vínculo del documento.

Eliminación de los vínculos de documentos

Puede quitar los vínculos de un documento de conocimiento no publicado, por ejemplo una relación principal-secundario. Si el documento ya está publicado, ábralo en modo de edición o reproceso para quitar los vínculos de documentos.

Procedimiento para quitar un vínculo de documento

1. Abra el documento de conocimiento.
Aparecerá el documento.
2. Haga clic en Editar.
Aparecerá la página Actualizar documento.
3. Seleccione la ficha Conocimiento relacionado.
Aparecerá la página Categorías.
4. Vaya al panel Vínculos de documento.
5. Seleccione la opción *Quitar este vínculo* del menú contextual para quitar el vínculo.
Se quitan los vínculos de documentos.

Categorías de conocimientos

Los documentos de conocimiento se organizan en *categorías del conocimiento*. Los técnicos de conocimiento, gestores de conocimientos y administradores pueden gestionar las categorías. Cada uno de estos individuos utiliza Gestión del conocimiento para crear, copiar y modificar categorías. Sin embargo, solamente los gestores de conocimientos y los administradores pueden suprimir categorías. Al construir la estructura de categorías en Categorías del conocimiento, está creando la estructura jerárquica que los empleados, clientes y analistas de Service Desk utilizan para desplazarse a los documentos pertinentes.

Asigne cada documento a una categoría primaria. Por ejemplo, cualquier conocimiento relacionado con Microsoft Word se debe agregar a la categoría de Microsoft Word. Además, Gestión del conocimiento permite asociar un documento con varias categorías secundarias y otros documentos. De esta manera, un documento se puede clasificar en distintas categorías aplicables y puede proporcionar resultados de búsqueda más satisfactorios.

La estructura de categorías desempeña las siguientes funciones:

- Organiza las soluciones de conocimiento en grupos fáciles de gestionar.
- Facilita la asignación de derechos de acceso.

- Permite buscar soluciones mediante la opción Preguntas frecuentes/Examinar.

Para utilizar la funcionalidad de exploración de categorías a partir de un incidente, el área de incidentes y la categoría de conocimiento deben coincidir. Cuando se crea un incidente basado en un documento de conocimiento, la categoría de documento establece el área de incidente; por lo tanto, la categoría y el área siempre coinciden.

- Crea un vínculo de documento: aparece un vínculo *Ver también* al visualizar cualquiera de los documentos vinculados. El vínculo *Ver también* permite ir directamente de un documento vinculado a otro.

Creación de categorías del conocimiento

En cada categoría se definen las propiedades que identifican los atributos o las cualidades que se deben asociar a los partes y, además, se crea un workflow que identifica todas las tareas necesarias para concluir los partes.

Puede utilizar categorías para especificar valores predeterminados para ciertos campos de los tickets, o bien asociar automáticamente un nivel de servicio a los tickets mediante la asignación de un tipo de servicio predeterminado a las categorías. Siempre que los analistas hayan asignado una categoría a un ticket, toda la información relacionada con dicha categoría se asocia automáticamente con el ticket.

Nota: Si está utilizando multicitente, aparece una lista desplegable de clientes en el filtro de búsqueda del documento de conocimiento. Si selecciona <vacío> en esta lista desplegable, la búsqueda es pública. También aparece una columna de cliente en la página de lista.

Procedimiento para crear una categoría

1. En la ficha Administración, vaya a Conocimiento, Categorías del conocimiento.
Aparecerá la página Categorías del conocimiento.
2. Haga clic con el botón secundario en la categoría en la cual desea crear la categoría. Seleccione Nueva categoría en el menú contextual.
Se abre la página Crear nueva categoría en la ficha Contenido.
3. Rellene los campos (see page 866) según corresponda.
4. Haga clic en Permisos.
Aparecerá la ficha Permisos.

5. Seleccione una de las opciones de permisos siguientes para la categoría:

Heredar del principal

Especifica que la nueva categoría tiene los mismos valores de permisos que su categoría principal.

Nota: La opción Heredar del principal no está disponible si selecciona la categoría superior antes de abrir la página Crear categoría.

Control por grupo

Especifica permisos de categoría para que los grupos tengan acceso de lectura o escritura a la categoría.

Control por rol

Especifica permisos de categoría para que los roles tengan acceso de lectura o escritura a la categoría.

Nota: Si cambia los controles, como cambiar los permisos de categoría de grupo a rol, aparece una advertencia que indica que los permisos anteriores se suprimen de esa categoría.

Conceder permiso de escritura a todos los usuarios

Especifica que todos los usuarios tienen acceso de escritura a la categoría. El acceso de escritura indica que se puede editar y eliminar esta categoría.

Nota: La casilla de verificación Conceder permiso de lectura a todos los usuarios se activa automáticamente al seleccionar la casilla de verificación Conceder permiso de escritura a todos los usuarios.

Conceder permiso de lectura a todos los usuarios

Especifica que todos los usuarios tienen acceso de lectura a la categoría. El permiso de lectura indica que se puede ver la categoría pero no editarla ni eliminarla. Los usuarios con derechos administrativos pueden editar una carpeta aunque su grupo de permisos asociado no se lo permita. Si un usuario pertenece a varios grupos de permisos con distintos niveles de acceso a la categoría, el usuario obtiene el mayor nivel de acceso disponible (por ejemplo, si un grupo tiene sólo acceso de lectura y el otro lo tiene de escritura, el usuario obtiene acceso de escritura).

Nota: La casilla de verificación Conceder permiso de lectura a todos los usuarios se activa automáticamente al seleccionar la casilla de verificación Conceder permiso de escritura a todos los usuarios.

Importante: cuando concede permisos para Todos, el acceso por rol o grupo es el mismo. Si selecciona Todos y Control por rol, después de guardar los permisos, el Control por grupo se activa.

6. (Opcional) Especificar permisos de lectura y escritura para grupos o roles específicos de las listas Disponible y Seleccionado.

Puede usar esta opción para gestionar los grupos o roles que tienen acceso de lectura o escritura a la categoría. Puede seleccionar uno o más roles o grupos de permisos de la lista Grupos/roles disponibles y, a continuación, usar los botones Agregar y Eliminar para mover los roles o grupos seleccionados a las listas Grupos/roles con permiso de escritura y Grupos/roles con permiso de lectura.

7. Haga clic en Guardar.

Aparecerá la página Detalles de categoría.

8. Haga clic en Cerrar ventana.

El panel Categorías del conocimiento se actualiza para incluir la nueva categoría.

Más información:

[Campos de categoría](#) (en la página 866)

Campos de categoría

Título

Establece el nombre de la categoría.

Descripción

Describe la categoría.

Propietario de la categoría

Indica la persona responsable de la categoría. Si un contacto está definido como el propietario de una categoría, tendrá un vínculo en la tarjeta de informes de conocimiento denominado Mis categorías, desde el que podrá ver estadísticas relacionadas con esa categoría y los documentos que contiene. Esta persona es también el propietario predeterminado de los nuevos documentos de la categoría cuando el usuario que crea los documentos no es un analista, o cuando un analista crea los documentos y selecciona la opción Asignar a propietario de la categoría.

Plantilla de documentos

Define la plantilla de documento que se debe utilizar en todos los documentos asociados a esta categoría. La opción <vacío> supone que no se ha definido ninguna; pero, de forma predeterminada, se usará la plantilla integrada.

Plantilla de procesos de aprobación

Define la plantilla predeterminada que se debe utilizar en el proceso de aprobación de todos los documentos asociados a esta categoría. La plantilla de procesos de aprobación define los pasos del workflow que debe recorrer un documento antes de su publicación. El valor predeterminado es <vacío>, lo que indica que se utilizará la plantilla predeterminada de la aplicación.

Permitir crear foros en esta categoría

Especifica si los analistas pueden crear foros dentro de esta categoría.

Área de solicitud/incidente/problema

Designa un área de solicitud/incidente/problema definida por el administrador para designar un área de responsabilidad. Puede hacer clic en el icono de búsqueda para seleccionar entre las áreas disponibles.

Categoría de incidencias

Designa una categoría de incidencia definida por el administrador para designar un área de responsabilidad. Puede hacer clic en el icono de búsqueda para seleccionar entre las áreas disponibles.

Modificación de categorías

La categoría se puede modificar en el entorno de Gestión del conocimiento. Las categorías determinan el contenido de las órdenes de cambio y las incidencias después de su creación. En cada categoría se definen las propiedades que identifican los atributos o las cualidades que se deben asociar a los partes y, además, se crea un workflow que identifica todas las tareas necesarias para concluir los partes.

Puede utilizar categorías para especificar valores predeterminados para ciertos campos de los tickets, o bien asociar automáticamente un nivel de servicio a los tickets mediante la asignación de un tipo de servicio predeterminado a las categorías. Siempre que los analistas hayan asignado una categoría a un ticket, toda la información relacionada con dicha categoría se asocia automáticamente con el ticket.

Procedimiento para modificar una categoría

1. En la ficha Administración, vaya a Conocimiento, Categorías del conocimiento.
Aparecerá la página Categorías del conocimiento.
2. Haga clic con el botón derecho en la categoría que desee modificar y seleccione Editar categoría en el menú contextual.

Se abre la página Actualizar categoría en la ficha Contenido.

Nota: No se puede eliminar o modificar la categoría superior.

3. Actualice uno o más campos (see page 866)según sea necesario.
4. Haga clic en Permisos.
Aparecerá la ficha Permisos.
5. Seleccione una de las opciones de permisos siguientes para la categoría:

Heredar del principal

Especifica que la nueva categoría tiene los mismos valores de permisos que su categoría principal.

Nota: La opción Heredar del principal no está disponible si selecciona la categoría superior antes de abrir la página Crear categoría.

Control por grupo

Especifica permisos de categoría para que los grupos tengan acceso de lectura o escritura a la categoría.

Control por rol

Especifica permisos de categoría para que los roles tengan acceso de lectura o escritura a la categoría. Si selecciona Todos y Control por rol, después de guardar los permisos, el Control por grupo queda seleccionado.

Nota: Si cambia los controles, como cambiar los permisos de categoría de grupo a rol, aparece una advertencia que indica que los permisos anteriores se suprimen de esa categoría.

6. (Opcional) Especificar los permisos de lectura y escritura para la categoría.
Puede usar esta opción para gestionar los grupos o roles que tienen acceso de lectura o escritura a la categoría. Si selecciona esta opción, la página se actualizará para incluir las casillas de verificación (see page 871) Conceder permiso de escritura a todos los usuarios y Conceder permiso de lectura a todos los usuarios.
7. Haga clic en Guardar.
La categoría modificada aparecerá en la página Lista de categorías del conocimiento.

Eliminación de categorías

Puede quitar una categoría de la estructura de categorías de conocimientos. Cuando elimina una categoría, puede especificar si desea quitar las subcategorías de la categoría seleccionada y todos los vínculos de documentos asociados.

Nota: Esta función sólo está disponible para administradores del sistema y gestores de conocimiento.

Para eliminar una categoría:

1. En la ficha Administración, vaya a Conocimiento, Categorías del conocimiento.

Aparecerá la página Categorías del conocimiento.

2. Haga clic con el botón derecho en la categoría que desee eliminar y seleccione Eliminar categoría en el menú contextual.

Aparecerá la página Eliminar categoría.

Nota: No se puede eliminar o modificar la categoría superior.

3. (Opcional) Realice *una* de las siguientes acciones:

- Marque la casilla de verificación Incluir subcategorías para eliminar todas las subcategorías de la categoría seleccionada.
- Quite la marca de la casilla de verificación Incluir subcategorías para mover las subcategorías de la categoría seleccionada a la categoría principal más próxima disponible.

4. (Opcional) Realice *una* de las siguientes acciones:

- Marque la casilla de verificación Incluir documentos para eliminar los documentos que se encuentren en la categoría seleccionada. Al marcar la casilla de verificación Incluir documentos, aparecen las siguientes opciones:
 - **Eliminar documentos vinculados por categoría principal solamente:** Elimina sólo documentos cuya categoría seleccionada aparezca en el panel Categorías del conocimiento como la categoría principal del documento.
 - **Eliminar todos los documentos vinculados a la categoría:** Elimina todos los documentos de la categoría seleccionada.
- Marque la casilla de verificación Incluir documentos para mover los documentos de la categoría seleccionada a la categoría principal más próxima disponible.

Haga clic en OK.

El producto suprime la categoría seleccionada y se actualiza el panel Categorías del conocimiento.

Cómo mover una categoría

Puede mover una categoría, sus subcategorías y todos los vínculos de documentos asociados de la ubicación actual a otra categoría.

Nota: Esta función sólo está disponible cuando Gestión del conocimiento está instalado.

Procedimiento para cortar y pegar una categoría

1. En la ficha Administración, vaya a Conocimiento, Categorías del conocimiento.
Aparecerá la página Categorías del conocimiento.
2. Haga clic con el botón derecho en la categoría que desee mover y seleccione Cortar categoría en el menú contextual.
El producto coloca la categoría seleccionada, sus subcategorías y todos los vínculos de documentos en memoria.
3. Haga clic con el botón secundario en la categoría en la que desee pegar la información que ha cortado y, a continuación, seleccione Pegar categoría en el menú contextual.
La categoría cortada se mueve de su ubicación original para posicionarse debajo de la categoría seleccionada. El panel Categorías del conocimiento se actualiza para mostrar la nueva estructura de categorías.

Copiar categorías con vínculos de documentos

Puede colocar la copia de una categoría, sus subcategorías y todos los vínculos de documentos en otra categoría, sin quitar la selección de su ubicación original.

Procedimiento para copiar y pegar una categoría con vínculos de documentos

1. En la ficha Administración, vaya a Conocimiento, Categorías del conocimiento.
Aparecerá la página Categorías del conocimiento.
2. Haga clic con el botón derecho en la categoría que desee copiar y seleccione Copiar categoría con vínculos de documentos en el menú contextual.
El producto coloca la categoría seleccionada, sus subcategorías y todos los vínculos de documentos en memoria.
3. Haga clic con el botón secundario en la categoría en la que desee pegar la información copiada y, a continuación, seleccione Pegar categoría en el menú contextual.
La información copiada aparece debajo de la categoría seleccionada. El panel Categorías del conocimiento se actualiza para mostrar la nueva estructura de categorías.

Copiar categorías sin vínculos de documentos

Puede colocar la copia de una categoría y sus subcategorías en otra categoría, sin quitar la selección de su ubicación original, o sin copiar los vínculos de documentos asociados.

Procedimiento para copiar y pegar una categoría sin vínculos de documentos

1. En la ficha Administración, vaya a Conocimiento, Categorías del conocimiento.
Aparecerá la página Categorías del conocimiento.
2. Haga clic con el botón derecho en la categoría que desee copiar y seleccione Copiar categoría en el menú contextual.
El producto coloca la categoría seleccionada y sus subcategorías en memoria.
3. Haga clic con el botón secundario en la categoría en la que desee pegar la información copiada y, a continuación, seleccione Pegar categoría en el menú contextual.
La información copiada aparece debajo de la categoría seleccionada. El panel Categorías del conocimiento se actualiza para mostrar la nueva estructura de categorías.

Gestión de permisos de categorías

Puede gestionar permisos de categoría en el entorno de Gestión del conocimiento si concede permisos de lectura/escritura específicos en función del grupo o rol. Puede especificar quién puede ver, editar, suprimir o agregar subcategorías a una categoría.

Nota: Puede utilizar permisos de escritura vacíos para documentos y categorías. Se establecen permisos de escritura vacíos cuando no se seleccionan permisos de escritura. Solamente los usuarios con privilegios pueden modificar categorías y documentos con permisos de escritura vacíos.

Procedimiento para gestionar permisos de categorías

1. En la ficha Administración, vaya a Conocimiento, Categorías de conocimiento.
Aparecerá la página Categorías del conocimiento.
2. Haga clic con el botón secundario en la categoría bajo la cual desea crear la categoría y, a continuación, seleccione Nueva categoría en el menú contextual para gestionar los permisos de una nueva categoría.
La página Crear nueva categoría muestra la ficha Contenido.

3. Haga clic en Permisos.

Aparecerá la ficha Permisos.

4. Seleccione una de las opciones de permisos siguientes para la categoría:

Heredar del principal

Especifica que la nueva categoría tiene los mismos valores de permisos que su categoría principal.

Nota: Si selecciona la categoría superior antes de abrir la página Crear categoría, la opción Heredar del principal no está disponible.

Control por grupo

Especifica permisos de categoría para que los grupos tengan acceso de lectura o escritura a la categoría.

Control por rol

Especifica permisos de categoría para que los roles tengan acceso de lectura o escritura a la categoría.

Nota: Si cambia los controles, como establecer los permisos de categoría de grupo a rol, aparece una advertencia que indica que los permisos existentes se suprimen.

Conceder permiso de escritura a todos los usuarios

Especifica que todos los usuarios tienen acceso de escritura a la categoría. El acceso de escritura indica que se puede editar y eliminar esta categoría.

Nota: La casilla de verificación Conceder permiso de lectura a todos los usuarios se activa automáticamente al seleccionar la casilla de verificación Conceder permiso de escritura a todos los usuarios.

Conceder permiso de lectura a todos los usuarios

Especifica que todos los usuarios tienen acceso de lectura a la categoría. El permiso de lectura indica que se puede ver la categoría pero no editarla ni eliminarla. Los usuarios con derechos administrativos pueden editar una carpeta aunque su grupo de permisos asociado no se lo permita. Si un usuario pertenece a varios grupos de permisos con distintos niveles de acceso a la categoría, el usuario obtiene el mayor nivel de acceso disponible (por ejemplo, si un grupo tiene sólo acceso de lectura y el otro lo tiene de escritura, el usuario obtiene acceso de escritura).

Nota: La casilla de verificación Conceder permiso de lectura a todos los usuarios se activa automáticamente al seleccionar la casilla de verificación Conceder permiso de escritura a todos los usuarios.

Importante: cuando concede permisos para Todos, el acceso por rol o grupo es el mismo. Si selecciona Todos y Control por rol, después de guardar los permisos, el Control por grupo se activa.

5. Conceda permisos de lectura/escritura apropiados a roles o grupos específicos en las listas disponibles y seleccionadas.

Puede seleccionar uno o más roles o grupos de permisos de la lista Grupos/roles disponibles y, a continuación, usar los botones Agregar y Eliminar para mover los roles o grupos seleccionados a las listas Grupos/roles con permiso de escritura y Grupos/roles con permiso de lectura.

Nota: Todos los grupos o roles agregados a la lista de permisos se agregan automáticamente a la lista de permisos de lectura. Cuando activa la casilla de verificación Conceder permisos de lectura a todos los usuarios, no necesita agregar grupos o roles a la lista de permisos de lectura.

6. Haga clic en Guardar.

Aparecerá la página Detalles de categoría.

7. Haga clic en Cerrar ventana.

La categoría modificada aparecerá en el panel Categorías del conocimiento.

Informes y métricas

Puede controlar la eficacia de la base de conocimiento con las siguientes herramientas de generación de informes:

- Tarjeta de informes de conocimientos
- Informes basados en Web predefinidos para Gestión del conocimiento
- Formularios Web de informes basados en roles

Estas herramientas permiten ver estadísticas sobre la utilidad de los documentos y su eficacia para resolver problemas.

Más información:

[Tarjeta de informes de conocimientos](#) (en la página 873)

[Informes basados en Web](#) (en la página 875)

[Formularios Web de informes basados en roles](#) (en la página 875)

Tarjeta de informes de conocimientos

La tarjeta de informes de conocimientos muestra información sobre la contribución de conocimiento de cada usuario final y proporciona comentarios acerca de los documentos de conocimiento que son más efectivos. Esta información se puede utilizar para mejorar los procesos de creación de los documentos de conocimiento y proporcionar el mejor soporte para los usuarios finales en su entorno.

Definición de estadísticas de tarjetas de informes de conocimiento

Utilice la página Tarjeta de informes de conocimiento para definir la programación en la que el producto calcula y envía notificaciones sobre la tarjeta de informes de conocimiento y para definir el contenido de los correos electrónicos de notificación sobre la tarjeta de informes de conocimiento.

Nota: Las versiones de reproceso y los documentos retirados no aparecen cuando se ejecuta el cálculo de la tarjeta de informes de conocimiento.

Procedimiento para definir estadísticas de tarjetas de informes de conocimiento

1. En la ficha Administración, seleccione Conocimiento, Tarjeta de informes de conocimiento.

Se abrirá la página Tarjeta de informe.

2. Rellene los siguientes campos según sea necesario.

Última modificación

Ejecuta el cálculo de la tarjeta de informes.

Valor predeterminado: desactivada

Nota: Si no se ejecuta el cálculo y no se recopilan las estadísticas para presentar los datos, aparecerá el siguiente mensaje al especificar el comando Tarjeta de informes de conocimiento en la ficha Conocimiento del menú Ver: "Ejecute el cálculo de la tarjeta de informes".

Programación

Programa la tarjeta de informes.

- **El cálculo de la tarjeta de informes se ejecutará el xxx y se ejecutará cada xxx:** especifica la frecuencia con la que se vuelven a calcular las estadísticas de tarjetas de informes.
- **Las notificaciones por correo electrónico de tarjetas de informes se enviarán el xxx y se enviarán cada xxx:** especifica la frecuencia con la que se enviarán notificaciones de tarjetas de informes.

Valor predeterminado: Nunca

- **Los correos electrónicos de tarjetas de informes deben mostrar las estadísticas de los últimos xxx:** especifica la cantidad de tiempo durante la cual la notificación de la tarjeta de informes debe contener información. Este campo sólo está disponible cuando se selecciona cualquier valor menos Nunca en la lista Las notificaciones por correo electrónico de tarjetas de informes se enviarán cada xxx.

Valor predeterminado: 365 días

3. Haga clic en Guardar.

Se han definido las estadísticas de la tarjeta de informes de conocimiento.

Informes basados en Web

CA Business Intelligence instala un conjunto de informes de Gestión del conocimiento predefinidos. Estos informes se implementan automáticamente en el servidor de generación de informes de BusinessObjects después de la instalación de CA Service Desk Manager.

Los informes se desarrollan mediante BusinessObjects Web Intelligence o Crystal Reports. Los usuarios autorizados pueden visualizar los informes en la ficha Informes de CA Service Desk Manager.

Formularios Web de informes basados en roles

Puede definir los formularios Web de los informes que aparecen cuando un gestor o analista autorizado hacen clic en el icono Lista de informes en la ficha Informes.

Los formularios Web de los informes se gestionan mediante la lista de roles en la siguiente ubicación: Administración, Gestión de roles y seguridad, Gestión de roles.

Búsqueda

La función Búsqueda permite a los administradores ejecutar las siguientes tareas:

- Gestionar el motor de búsqueda de Gestión del conocimiento y definir los valores que se deben utilizar para gestionar las palabras irrelevantes, los términos especiales y los sinónimos que se excluyen o incluyen en las búsquedas.
- Definir los valores que se utilizan para analizar los documentos.
- Definir los valores de búsqueda predeterminados.

- Crear "documentos recomendados" que se muestran en los resultados de la búsqueda. El listado dinámico de preguntas frecuentes se utiliza para hacer llegar los documentos recomendados a los usuarios.

Nota: Un documento puede tener permisos diferentes que sus adjuntos vinculados.

- Cambiar al motor de búsqueda FAST (si está instalado).

Véase también

[Motor de búsqueda de KT](#) (en la página 876)

[Búsqueda FAST ESP](#) (en la página 889)

[Documentos recomendados](#) (en la página 892)

[Configuración de los valores de búsqueda predeterminados](#) (en la página 896)

Motor de búsqueda de KT

Después de haber instalado CA Service Desk Manager, el motor de búsqueda de KT se configura como predeterminado. Las búsquedas de la base de conocimiento se limitan a documentos de conocimiento. El motor de búsqueda se encuentra en la ficha Administración, Conocimiento, Buscar, nodo Motor de búsqueda de KT.

El nodo Motor de búsqueda de KT permite gestionar las siguientes opciones:

- Palabras irrelevantes
- Términos especiales
- Sinónimos

Más información:

[Utiliza la búsqueda de Gestión del conocimiento](#) (en la página 876)

Utiliza la búsqueda de Gestión del conocimiento

Tras instalar CA Service Desk Manager, se configura el motor de búsqueda de Gestión del conocimiento como el motor de búsqueda predeterminado. Las búsquedas de la base de conocimiento se limitan a documentos de conocimiento.

Puede definir la accesibilidad y los valores predeterminados de todos los orígenes de conocimiento basados en un rol de usuario. De forma predeterminada, todos los roles de usuario pueden realizar búsquedas en los documentos de conocimiento.

Si CA Service Desk Manager está configurado para la búsqueda de FAST ESP, puede cambiar al motor de búsqueda predeterminado en el gestor de opciones.

Procedimiento para utilizar la búsqueda de Gestión del conocimiento

1. Haga clic en la ficha Administración.
Aparecerá la consola de administración.
2. Haga clic en Gestor de opciones, Motor de búsqueda.
Aparecerá la lista de opciones.
3. Haga clic en ebr_version.
Aparecerá la página Detalles de opciones.
Haga clic en Editar. Aparece la página Actualizar opciones.
4. Seleccione Motor de búsqueda de KT.
5. Haga clic en Guardar, Actualizar.
La página Detalle de opciones se actualiza con la selección.
6. Haga clic en Cerrar ventana.

Nota: Para obtener información sobre la instalación y configuración de FAST ESP, consulte la *Guía de implementación*.

Véase también

[Palabras irrelevantes, sinónimos y términos especiales](#) (en la página 878)
[Creación de palabras irrelevantes](#) (en la página 879)
[Edición de palabras irrelevantes](#) (en la página 880)
[Visualización de palabras irrelevantes](#) (en la página 880)
[Creación de términos especiales](#) (en la página 881)
[Edición de términos especiales](#) (en la página 881)
[Visualización de términos especiales](#) (en la página 882)
[Creación de sinónimos](#) (en la página 883)
[Visualización de sinónimos](#) (en la página 883)
[Edición de sinónimos](#) (en la página 884)
[Valores de análisis](#) (en la página 885)

Palabras irrelevantes, sinónimos y términos especiales

Nota: Las palabras irrelevantes, los sinónimos y los términos especiales sólo están disponibles con el motor de búsqueda predeterminado. El motor de búsqueda FAST ESP opcional proporciona un mecanismo de detección interno para gestionar palabras irrelevantes, sinónimos y términos especiales. Para obtener información sobre la implementación, consulte la documentación de FAST ESP.

Puede definir palabras (sinónimos, palabras irrelevantes y términos especiales) que afectan a las búsquedas por lenguaje natural y por palabras clave realizadas en CA Service Desk Manager. La adición o supresión de los términos siguientes tiene un efecto significativo sobre los resultados de la búsqueda devueltos al usuario:

Palabras irrelevantes

Especifica palabras que, por lo general, no aportan nada al proceso de búsqueda y que, por consiguiente, se pueden ignorar. Por ejemplo, los artículos (un, una, el, la) o las conjunciones (y, o) se suelen identificar como palabras irrelevantes. Utilice la página Lista de palabras irrelevantes para especificar palabras que el producto puede omitir en documentos y consultas sin que afecte a los resultados de búsqueda.

Términos especiales

Especifica un término que desea identificar como una sola palabra durante el proceso de búsqueda, aunque puede estar formado por varias palabras o contener caracteres especiales. Por ejemplo, las palabras que contienen algún carácter que no sea alfanumérico como la barra (/) en TCP/IP, o el guión bajo en SERVIDOR_LOCAL, se pueden agregar como términos especiales. Al evaluar las palabras que se deben definir, tenga en cuenta las palabras válidas que puedan ser divididas en el proceso de búsqueda por tener algún carácter que no sea alfanumérico.

Sinónimos

Especifica una palabra que tiene el mismo significado que otra. Puede agregar sinónimos de modo que, cuando un usuario busque una palabra determinada y exista un sinónimo correspondiente para esa palabra en la base de conocimiento, la información se pueda encontrar. Es posible definir varios sinónimos para la misma palabra. El sistema crea automáticamente sinónimos inversos a partir de las palabras clave definidas. Por ejemplo, si define equipo como un sinónimo de la palabra PC, PC se convierte automáticamente en un sinónimo de la palabra equipo. Utilice la página Lista de sinónimos para especificar pares palabra clave/sinónimo que el producto debe utilizar indistintamente al analizar los documentos y las consultas. Los pares palabra clave/sinónimo pueden mejorar los resultados de la búsqueda.

Nota: Después de crear, modificar o eliminar palabras irrelevantes, términos especiales, sinónimos o valores de análisis, use la utilidad de reindización de conocimientos proporcionada con el producto para reindizar la base de conocimiento.

Creación de palabras irrelevantes

Utilice la página Crear nueva palabra irrelevante para agregar una palabra nueva a la lista de palabras que el producto puede omitir en documentos y consultas sin que se vean afectados los resultados de la búsqueda.

Procedimiento para crear una palabra irrelevante

1. En la ficha Administración, seleccione Conocimiento, Buscar, Motor de búsqueda de KT, Palabras irrelevantes.

Aparece la página Lista de palabras irrelevantes.

2. Haga clic en Crear nuevo.
3. Aparece la página de detalles Crear nueva palabra irrelevante.
4. En el campo Palabra irrelevante, escriba la palabra que desee definir como irrelevante.

Nota: No puede definirse una palabra irrelevante que ya exista como sinónimo o palabra clave.

5. Haga clic en Guardar.

Aparece la nueva palabra irrelevante en la página Lista de palabras irrelevantes. Puede hacer el botón Editar para actualizar la nueva palabra irrelevante.

Nota: Después de crear, modificar o eliminar palabras irrelevantes, términos especiales, sinónimos o valores de análisis, use la utilidad de reindización de conocimientos proporcionada con el producto para reindizar la base de conocimiento.

Edición de palabras irrelevantes

En la página Lista de palabras irrelevantes puede editar una palabra irrelevante que ya ha sido creada.

Nota: Después de crear, modificar o eliminar palabras irrelevantes, términos especiales, sinónimos o valores de análisis, use la utilidad de reindización de conocimientos proporcionada con el producto para reindizar la base de conocimiento.

Procedimiento para editar una palabra irrelevante

1. Haga clic con el botón secundario en la palabra irrelevante deseada en la lista Palabras irrelevantes y seleccione Propiedades en el menú contextual.

Se abre la página Actualización de palabras irrelevantes.

2. Escriba las ediciones en el campo Palabra irrelevante.

Nota: No puede definirse una palabra irrelevante que ya exista como sinónimo o palabra clave.

3. Haga clic en Guardar.

Aparece la palabra irrelevante actualizada en la página Lista de palabras irrelevantes.

Nota: Después de definir, modificar o eliminar palabras irrelevantes, términos especiales, sinónimos o valores de análisis, use la utilidad de reindización de conocimientos proporcionada con el producto para reindizar la base de conocimiento.

Visualización de palabras irrelevantes

Puede ver la información de resumen de cada palabra irrelevante en la página Lista de palabras irrelevantes.

Para mostrar la información de resumen de cada palabra irrelevante, seleccione la ficha Administración y, a continuación, Conocimiento, Buscar, Motor de Búsqueda de KT, Palabras irrelevantes.

Aparece la página Lista de palabras irrelevantes y contiene los campos siguientes:

Palabra irrelevante

Define una palabra irrelevante que se utilizará en las búsquedas. Este campo sólo se muestra al hacer clic en Mostrar filtro.

Argumentos de búsqueda adicionales

Define otros criterios para incluirlos en la búsqueda. Este campo sólo aparece cuando se hace clic en el vínculo Más de la página Búsqueda de conocimiento.

Lista de palabras irrelevantes

Muestra palabras que se utilizarán para filtrar los resultados de las búsquedas. La lista se muestra si se hace clic en el botón Buscar. Si ha introducido una palabra en el campo Palabra irrelevante, en la lista sólo se muestra esa palabra. Si no ha introducido nada en el campo Palabra irrelevante, la lista mostrará todas las palabras irrelevantes definidas para el producto.

En la página Lista de palabras irrelevantes, puede ejecutar las siguientes tareas:

- Creación de palabras irrelevantes (see page 879)
- Edición de palabras irrelevantes (see page 880)

Creación de términos especiales

Utiliza la página Crear nuevo término especial para especificar una palabra o frase que el producto debe considerar como palabras clave únicas al analizar los documentos y las consultas.

Procedimiento para crear un término especial

1. En la ficha Administración, vaya a Conocimiento, Buscar, Motor de búsqueda de KT, Términos especiales.
Aparece la página Lista de términos especiales.
2. Haga clic en Crear nuevo.
Aparece la página Crear nuevo término especial.
3. Escriba en el cuadro Término especial la palabra o frase que desee definir como término especial.
4. Haga clic en Guardar.

Se cierra la página Crear nuevo término especial y se abre la página Detalles de término especial para que pueda revisar la palabra o frase que ha agregado. Puede utilizar el botón Editar para actualizar el nuevo término. Aparece el nuevo término especial en la página Lista de términos especiales.

Edición de términos especiales

Puede editar un término especial.

Procedimiento para editar un término especial

1. Haga clic con el botón secundario en el término que desee editar en la lista, y seleccione Editar en el menú contextual.
Aparece la página Actualizar término especial.

2. Escriba en el cuadro Término especial la palabra o frase que desee definir como término especial.
3. Haga clic en Guardar.

Se cierra la página Actualizar término especial y se abre la página Detalles de término especial para que pueda revisar la palabra o frase que ha agregado. El término actualizado aparece en la página Lista de términos especiales.

Visualización de términos especiales

Puede ver la información de resumen de cada término especial.

Para ver términos especiales, seleccione la ficha Administración y, a continuación, Conocimiento, Buscar, Motor de búsqueda de KT, Términos especiales.

Aparece la página Lista de términos especiales, y puede utilizar los campos siguientes para modificar los términos que aparecen de forma predeterminada, o definir sus propios términos:

Término especial

Define un término especial que se utilizará en las búsquedas. Este campo sólo se muestra al hacer clic en Mostrar filtro.

Argumentos de búsqueda adicionales

Define otros criterios para incluirlos en la búsqueda. Este campo sólo se muestra cuando se hace clic en el vínculo Más del panel Búsqueda de conocimientos.

Términos especiales

Muestra las palabras o frases que contienen espacios o caracteres (como guiones, barras, etc.) que el producto considera como palabras clave únicas al analizar las consultas. Si ha introducido una palabra en el campo Término especial antes de hacer clic en Buscar, la lista sólo mostrará la palabra especificada. Si no ha introducido nada en el campo Término especial, la lista mostrará todos los términos especiales definidos para el producto.

En la página Lista de palabras irrelevantes, puede ejecutar las siguientes tareas:

- Creación de un término especial (see page 881)
- Edición de un término especial (see page 881)

Creación de sinónimos

Los sinónimos son palabras o frases que tienen un significado idéntico o parecido al de la palabra clave a la que están asociados.

Si define un nuevo sinónimo complejo (es decir, un sinónimo que contiene varias palabras separadas por espacios u otros delimitadores), cree también un término especial idéntico para que el producto pueda considerar el sinónimo como una entidad única. Por ejemplo, si define "Computer Associates" como sinónimo de "CA", también debe definir "Computer Associates" como término especial.

Nota: No se puede definir un sinónimo o palabra clave que ya exista como palabra irrelevante.

Procedimiento para crear un sinónimo

1. En la ficha Administración, vaya a Conocimiento, Buscar, Motor de búsqueda de KT, Términos especiales.
Aparecerá la página Lista de sinónimos.
2. Haga clic en Crear nuevo.
Aparece la página Crear nuevos sinónimos.
3. En el campo Sinónimos escriba la palabra o frase que desee definir como término especial.
4. Haga clic en Guardar.
Se cierra la página Crear sinónimos y se abre la página Detalles de sinónimos para que pueda revisar la palabra o frase que ha agregado.
Aparece el nuevo sinónimo en la página Lista de sinónimos.

Visualización de sinónimos

Puede ver la información de resumen de cada sinónimo.

Para ver sinónimos, seleccione la ficha Administración y, a continuación, Conocimiento, Buscar, Motor de Búsqueda de KT, Sinónimos.

Aparece la página Lista de sinónimos, y puede modificar las palabras clave que aparecen de forma predeterminada, o definir sus propias palabras utilizando los campos siguientes:

Palabra clave

Define una palabra clave que se utilizará en las búsquedas. Este campo sólo se muestra al hacer clic en Mostrar filtro.

Sinónimo

Define un sinónimo que se utilizará en las búsquedas. Este campo sólo se muestra al hacer clic en Mostrar filtro.

Argumentos de búsqueda adicionales

Define otros criterios para incluirlos en la búsqueda. Este campo sólo se muestra cuando se hace clic en el vínculo Más del panel Búsqueda de conocimientos.

Lista de sinónimos

Muestra los pares palabra clave/sinónimo definidos en el producto. En la columna Sinónimo se muestra uno o más sinónimos de cada palabra clave que aparece en la columna Palabra clave.

En la página Lista de sinónimos, puede ejecutar las siguientes tareas:

- Creación de un sinónimo (see page 883)
- Edición de un sinónimo (see page 884)

Edición de sinónimos

Puede editar un sinónimo.

Procedimiento para editar un sinónimo

1. Haga clic con el botón secundario en el término que desee editar en la lista, y seleccione Editar en el menú contextual.
Aparecerá la página Actualizar sinónimo.
2. En el campo Sinónimo, escriba la palabra o frase que desee definir como término especial.
3. Haga clic en Guardar.

Se cierra la página Actualizar sinónimo y se abre la página Detalles de sinónimo para que pueda revisar la palabra o frase que ha agregado. Aparece el término actualizado en la página Lista de sinónimos.

Valores de análisis

Nota: La función Valores de análisis sólo está disponible con el motor de búsqueda de KT predeterminado.

Al publicar un documento en la base de conocimientos, el producto analiza la información de los campos Título, Resumen, Problema y Resolución del documento y los transforma en palabras clave. Cuando un usuario busca en la base de conocimiento, el producto compara las palabras clave de la consulta del usuario con las palabras clave analizadas en la base de conocimiento para generar una lista de resultados. La página Valores de análisis permite definir los valores que se utilizan para analizar los documentos de la base de conocimiento.

Definición de valores de análisis

Al publicar un documento en la base de conocimientos, el producto analiza la información de los campos Título, Resumen, Problema y Resolución del documento y los transforma en palabras clave. Cuando un usuario busca en la base de conocimiento, el producto compara las palabras clave de la consulta del usuario con las palabras clave analizadas en la base de conocimiento para generar una lista de resultados.

Nota: FAST ESP tiene su propio mecanismo de optimización interno para devolver resultados relevantes. Por lo tanto, los valores de análisis (excepto el rango de caracteres válido) no aparecen en la interfaz de administración de Gestión del conocimiento cuando se ha instalado y configurado el motor de búsqueda FAST ESP opcional.

Para definir los valores utilizados para analizar documentos en la base de conocimiento, vaya a la ficha Administración en Conocimiento, Buscar, Valores de análisis.

Aparece Valores de análisis, y puede utilizar los campos siguientes para definir los valores:

Máximo de palabras clave buscadas

Define el número máximo de palabras clave que se extraerán cuando el producto analice el texto de búsqueda.

Valor predeterminado: 20

Nota: El intervalo válido es 1-100, de forma que el administrador de conocimientos de Service Desk pueda cambiar el valor dentro de este intervalo, según las necesidades de la búsqueda y los parámetros de una base de datos de conocimientos específica. Utilice menos palabras clave de búsqueda para obtener un rendimiento mayor.

Idioma

Especifica el tipo de idioma que se va a utilizar en el proceso de análisis. Seleccione uno de los siguientes valores:

Inglés

Realiza ciertos tipos de procesamientos específicos del español (por ejemplo, la conversión a singular de los términos de búsqueda en plural) durante las búsquedas, si procede.

Otros europeos

Realiza procesamientos específicos de países europeos durante las búsquedas.

Coreano

Realiza procesamientos específicos del coreano durante las búsquedas.

Otro: Lejano Oriente

Realiza procesamiento para otros idiomas de Lejano Oriente durante la búsqueda.

Nota: Cuando se encuentre en el entorno operativo chino, japonés o coreano, verifique que entiende los enfoques de análisis disponibles, y las limitaciones de los idiomas de conjuntos de caracteres de varios bytes (MBCS) (see page 888), antes de implementar el sistema Gestión del conocimiento para asegurarse que las expectativas de usuario se definen apropiadamente.

Rango de caracteres válido

Define el intervalo de caracteres alfanuméricos que se deben considerar válidos a la hora de analizar los campos Título, Resumen, Problema y Resolución de un documento. El producto considera el resto de caracteres como separadores.

Nota: Si selecciona Sí en la lista Reconocer términos especiales, el producto no analiza las palabras y frases definidas como términos especiales.

Valor predeterminado: a-z, que indica que los caracteres alfabéticos de la a a la z se consideran caracteres válidos para el análisis.

El campo Rango de caracteres válido contiene las letras adecuadas utilizadas por el análisis. Se eliminarán las letras que no se encuentren en el campo Rango de caracteres válido.

Los valores recomendados para los distintos idiomas son los siguientes:

Idioma	Rango de caracteres válido
Alemán	a-zäöüß
Español	a-záéíóúüñ
Francés	a-zàâçéèëïîôùû
Portugués (Brasil)	a-zãäãçéêíóü
Italiano	a-zàèéìü
Chino simplificado	a-z
Japonés	a-z
Chino tradicional	a-z
Coreano	a-z

Nota: El idioma japonés contiene el rango "a-z" más una lista de caracteres katakana válidos sin incluir los signos de puntuación.

Eliminar palabras similares

Especifica si el producto debe eliminar palabras claves de estructura similar de los grupos utilizados en una búsqueda. Puede seleccionar uno de los siguientes valores:

Sí

Elimina las palabras clave de estructura similar de los criterios de búsqueda.

Nota: Si selecciona Sí, el producto también elimina las palabras similares al guardar o publicar el documento. Este valor puede determinar si un documento puede buscarse cuando el cuadro Eliminar palabras similares se haya definido como Sí. La palabra similar puede que no se haya indizado y utilizado en la búsqueda y recuperación posteriores del documento.

No

Mantiene las palabras clave de estructura similar en los criterios de búsqueda.

Predeterminado: No

Eliminar palabras irrelevantes

Especifica si el producto debe eliminar las palabras irrelevantes cuando analice los campos Título, Resumen, Problema y Resolución de un documento. Puede seleccionar uno de los siguientes valores:

Sí

Elimina las palabras irrelevantes de los criterios de búsqueda.

No

Mantiene las palabras irrelevantes en los criterios de búsqueda.

Predeterminado: Sí

Reconocer términos especiales

Especifica si el producto debe considerar los términos especiales como entidades únicas o varias palabras cuando analice los campos Título, Resumen, Problema y Resolución de un documento. Puede seleccionar uno de los siguientes valores:

Sí

Procesa los términos especiales como entidades únicas en los criterios de búsqueda.

No

Procesa las palabras que contienen términos especiales como entidades individuales en los criterios de búsqueda.

Predeterminado: Sí

Limitaciones de búsqueda de los conjuntos de caracteres de varios bytes (MBCS)

Asegúrese de entender los enfoques de análisis disponibles, y las limitaciones de los idiomas MBCS, antes de implementar el sistema Gestión del conocimiento para asegurarse de que las expectativas de usuario se definen apropiadamente. Esta limitación de las opciones de búsqueda repercute en las funciones de búsqueda que utilizan texto de idioma en japonés, chino o coreano en el sistema. El mecanismo de análisis de palabras utilizado por el mecanismo de búsqueda se controla en la página Valores de análisis (see page 885).

Para los valores de configuración en inglés, coreano y otros países europeos, el producto asume que las palabras están separadas por el punto, el espacio blanco, o ambos caracteres. Esta suposición permite que el texto del documento se separe en palabras específicas y que se ignoren las palabras irrelevantes y se aplican sinónimos y términos especiales conocidos para buscar términos.

Como alternativa, cuando se seleccionan valores de idioma del lejano oriente, la rutina de análisis utiliza un enfoque de análisis de carácter por carácter para ajustarse a algunos enfoques de texto de idioma del lejano oriente de no utilizar delimitadores de espacios en blanco entre las palabras. Esta definición le indica al analizador que asuma que cada carácter se considere como una palabra completa. La definición se aplica a todo el texto que se va a buscar. Debido a que los valores de idioma cambian la manera en que funciona el análisis de búsqueda, se debe recrear el índice de búsqueda completo al cambiar los valores de idioma a o desde lejano oriente.

Nota: FAST ESP es un motor de búsqueda opcional que proporciona soporte para idiomas de conjuntos de caracteres de varios bytes (MBCS) y permite superar estas limitaciones de búsqueda. Para obtener información sobre la configuración del motor de búsqueda FAST ESP, consulte la *Guía de implementación*.

Búsqueda FAST ESP

La búsqueda FAST ESP es un motor de búsqueda opcional que permite a los analistas y los gestores de conocimientos buscar los siguientes orígenes de conocimiento:

- Documentos de conocimiento con varios adjuntos
- Foros de analistas
- Archivos de conocimiento (.pdf, .zip, .xls, .exe, .html, .img, .msg, .ppt, .rtf, .txt, .avi, .doc y .xml)
- Contenido de texto libre (conocimiento desestructurado) referido a un problema o una resolución
- Incidencias del centro de servicio al usuario, incidentes, solicitudes, problemas y órdenes de cambio
- Sitios Web o sistemas de archivo. El motor de búsqueda cataloga e indiza el contenido que reside en los repositorios externos

El motor de búsqueda tiene las siguientes limitaciones:

- FAST solamente puede procesar dos consultas de búsqueda por segundo.
Nota: Para obtener información sobre cómo ampliar esta capacidad, póngase en contacto con Servicios de CA.
- El número máximo de documentos que se pueden indizar en la base de conocimiento es de 2.000.000.
- Nota: Un documento puede tener permisos diferentes que sus adjuntos vinculados.

De forma predeterminada, CA Service Desk Manager no está configurado para utilizar FAST ESP. Si ha instalado el motor de búsqueda FAST ESP, puede seleccionar ese motor de búsqueda como el predeterminado para realizar las búsquedas de Gestión del conocimiento. Los valores predeterminados del motor de búsqueda se definen en el gestor de opciones.

Nota: Para obtener información sobre la instalación y configuración de FAST ESP, consulte la *Guía de implementación*.

Uso del motor de búsqueda FAST

Si CA Service Desk Manager se ha configurado para utilizar el motor de búsqueda predeterminado, puede habilitar el motor de búsqueda FAST (si está instalado). El motor de búsqueda FAST proporciona capacidades de búsqueda adicionales que permite a los usuarios buscar soluciones de conocimiento mediante un sitio Web o un sistema de archivos, y mucho más.

Siga estos pasos en el servidor primario o secundario de CA Service Desk Manager.

Nota: Para obtener información sobre la instalación y configuración de FAST ESP, consulte la *Guía de implementación*.

Procedimiento para utilizar el motor de búsqueda FAST

1. Haga clic en la ficha Administración.
Aparecerá la consola de administración.
2. En el árbol a la izquierda, haga clic en Gestor de opciones, Motor de búsqueda.
Aparecerá la lista de opciones.
3. Especifique la configuración siguiente:

ebr_version

Especifica FAST [motor de búsqueda].

ebr_search_engine_baseport

Especifica el puerto base del servidor especializado en el cual está instalado el motor de búsqueda FAST ESP. Tenga en cuenta lo siguiente al especificar el puerto de base:

- Asegúrese de que el número de puerto que introduce aquí coincida con el puerto base especificado durante la instalación de FAST ESP (el puerto predeterminado es 13000).
- FAST ESP utiliza el puerto base para calcular puertos estáticos.

- En cada host, debería haber un espacio de 4000 puertos entre el puerto base de FAST ESP y la instalación de FAST ESP porque FAST ESP compensa sus puertos estáticos desde el puerto base (es decir, el número de puerto de la interfaz de administración es 16000).
- Asegúrese de que este intervalo de puertos no entre en conflicto con otros productos o servicios usados por el servidor.
- No puede utilizar puertos por debajo de 1024.
- Recomendamos que *no use* un puerto base en el intervalo de 23000 a 27000, porque el servidor de licencias siempre utiliza el número de puerto 27000.

Importante: todos los host deben tener acceso de red sin restricciones en el intervalo de puertos completo (por ejemplo, los puertos 13000 a 16999).

ebr_search_engine_host

Especifica el nombre de dominio completo o la dirección IP (recomendado) del servidor dedicado en el que está instalado el motor de búsqueda FAST ESP.

4. Haga clic en Guardar, Actualizar.
La página Detalle de opciones se actualiza con la selección.
5. Haga clic en Cerrar ventana.
6. Detenga e inicie el servicio denominado Servidor de CA Service Desk Manager.
7. Ejecute el comando *pdm_k_reindex (see page 1025) index factory:all* para indexar documentos de conocimiento y tickets en FAST ESP.

Importante: si detiene y reinicia los servicios de FAST ESP por cualquier motivo, también *debe* detener y reiniciar el daemon de indexación (bpeid_nxd). FAST ESP *debe* estar en ejecución para que el daemon se inicie. De lo contrario, se producirán errores en *stdlog* y al crear o buscar documentos de conocimiento.

Más información:

[pdm_k_reindex: utilidad de reindexación de conocimientos](#) (en la página 1025)

[Cuándo utilizar pdm_k_reindex](#) (en la página 1026)

[Utilice pdm_k_reindex con FAST ESP](#) (en la página 1028)

Opción Buscar similar

Se pueden buscar tickets similares en la ficha Conocimiento de los tickets, que incluyen Incidencias, Solicitudes, Incidentes, Problemas y Órdenes de cambio. La opción Buscar similar se habilita solamente cuando se instala FAST ESP. Esta funcionalidad permite buscar tickets similares utilizando el resumen y la descripción del ticket como una consulta de búsqueda. La búsqueda de tickets similares ayuda a evitar la creación de tickets redundantes en el entorno de soporte.

Importante: si quiere utilizar Buscar similar, debe ejecutar `pdm_k_reindex` (see page 1028) para sincronizar los documentos. También debe reindexar cada uno de los objetos de CA Service Desk Manager, como por ejemplo Solicitudes de llamada, Órdenes de cambio, etc.

Uso de la opción de búsqueda Buscar similar en tickets

Es posible realizar búsquedas de tickets similares en la ficha Conocimiento de un ticket, como por ejemplo un incidente. La opción Buscar similar se habilita solamente cuando se instala FAST ESP. El propósito de las búsquedas de tickets similares es evitar crear tickets redundantes en el entorno de soporte.

Procedimiento para encontrar tickets similares

1. Abra un ticket, como, por ejemplo, un incidente.
Aparecerá la página Detalles de incidente.
2. En la ficha de Conocimiento, haga clic en Buscar similar.
Aparece una lista de tickets similares, basada en el resumen y la descripción del incidente.

Documentos recomendados

Los usuarios de CA Service Desk Manager pueden especificar criterios sobre un elemento de interés y el motor de búsqueda busca los documentos de conocimiento coincidentes y los muestra en la página de resultados de la búsqueda como un conjunto de vínculos de "documentos recomendados". La consulta de búsqueda se puede expresar como una palabra clave o conjunto de palabras (frase) que identifica el concepto deseado que pueden contener uno o varios documentos.

La lista de documentos que coincide con los criterios de búsqueda se ordena y se clasifica (de mayor a menor) para colocar en el primer lugar de los resultados de la búsqueda los documentos más relevantes. La utilización de documentos recomendados ayuda a los usuarios a reducir el tiempo necesario de encontrar la información deseada.

Para proporcionar rápidamente un conjunto de documentos coincidentes clasificados según algunos criterios, el motor de búsqueda reúne los datos por el tipo de condición (frase, palabras clave o categoría), configurado por el administrador en la página Crear documentos recomendados.

Más información:

[Creación de documentos recomendados](#) (en la página 893)

[Edición de condiciones de documentos recomendados](#) (en la página 895)

[Visualización de documentos recomendados](#) (en la página 895)

[Búsqueda de documentos recomendados](#) (en la página 896)

Creación de documentos recomendados

Los administradores pueden crear documentos recomendados que los usuarios podrán encontrar al especificar criterios sobre un elemento de interés.

Nota: Si el multicliente está instalado, seleccione el cliente apropiado de la lista desplegable. La opción público (compartida) crea el objeto para todos los clientes.

Procedimiento para crear un documento recomendado

1. En la ficha Administración, vaya a Conocimiento, Buscar, Documentos recomendados.
Aparecerá la Lista de documentos recomendados.
2. Haga clic en Crear nuevo.
Aparece la página Crear nuevos documentos recomendados.
3. Rellene los siguientes campos según sea necesario.

Documento de conocimiento

Especifique un documento de conocimiento o haga clic en el icono de búsqueda para abrir la página Búsqueda de documentos de conocimiento.

Tipo de condición

Especifica un tipo de condición (see page 894) por el cual el motor de búsqueda ordena y busca coincidencias en el documento.

- Si el tipo de condición es Coincidencia completa, Frase exacta o Palabras clave, aparece un campo de texto. Puede introducir una frase o palabra clave que identifica el concepto que desea que contenga el documento.
- Si el tipo de condición es Categoría de conocimiento, aparece el vínculo Categoría de conocimiento. Puede especificar la categoría de conocimiento que desea asociar con este documento.

Abre el cuadro de diálogo Estado de acción, que muestra el estado de la tarea o el trabajo seleccionado, la fecha y la hora de la última ejecución y el número de ejecuciones.

Define el estado de este registro como activo o inactivo.

Haga clic en Guardar.

El nuevo documento recomendado se guarda en la base de conocimiento y aparece en la página Lista de documentos recomendados.

Campo de tipo de condición

El motor de búsqueda encuentra documentos según los tipos de condición siguientes:

Coincidencia completa

Busca documentos por la frase de búsqueda introducida en el texto de búsqueda. Sólo se produce una coincidencia cuando el motor de búsqueda encuentra todas las mismas palabras en una frase.

Frase exacta

Busca documentos por la frase exacta introducida en el texto de búsqueda. Sólo se produce una coincidencia cuando el motor de búsqueda encuentra en una frase el conjunto o secuencia de palabras exacto.

Palabras clave

Busca documentos por las palabras clave introducidas en el texto de búsqueda. Sólo se produce una coincidencia cuando el motor de búsqueda encuentra todas las palabras clave.

Categoría de conocimiento

Busca documentos por la categoría de conocimiento. Sólo se produce una coincidencia cuando un usuario explora una categoría configurada para documentos recomendados.

Edición de condiciones de documentos recomendados

Puede actualizar una condición de documento recomendado.

Procedimiento para editar condiciones de documentos recomendados

1. En la ficha Administración, vaya a Conocimiento, Buscar, Documentos recomendados.
Aparecerá la página Documentos recomendados.
2. Para editar una condición, haga clic con el botón secundario en el título de la columna Condición.
Aparecerá la página Actualizar documentos recomendados.
3. Rellene los campos según sea necesario.
4. Haga clic en Guardar.
La condición actualizada aparece en la lista Documentos recomendados.

Visualización de documentos recomendados

Puede ver la información de resumen de cada documento recomendado.

Para visualizar los documentos recomendados, en la ficha Administración, seleccione Buscar y, a continuación, Documentos recomendados.

Aparece la página Lista de documentos recomendados en la que se muestran las siguientes columnas:

Condición

Indica la condición por la cual el motor de búsqueda ordena y busca coincidencias en el documento.

Documento de conocimiento

Muestra los documentos en el conjunto de resultados.

Autor

Define un autor del documento de conocimiento.

Fecha de modificación

Muestra la fecha de la última modificación del documento.

En la página Lista de documentos recomendados, puede ejecutar las siguientes tareas:

- Creación de un documento recomendado (see page 893)
- Edición de condiciones de documentos recomendados (see page 895)
- Búsqueda de documentos recomendados (see page 896)

Búsqueda de documentos recomendados

Puede utilizar la función de búsqueda para filtrar la lista de documentos recomendados para que sólo se muestren los elementos que desea ver.

Nota: Si multiciente está instalado, la página de lista muestra la configuración de datos públicos y de clientes en el filtro de búsqueda. Los datos públicos se pueden excluir o incluir con los datos de clientes; sólo se buscan objetos públicos exclusivamente. En las páginas de detalles, seleccione el cliente apropiado de la lista. Si selecciona <vacío>, el objeto es público.

Procedimiento para buscar un documento recomendado

1. En la ficha Administración, vaya a Conocimiento, Buscar, Resultados recomendados.
Aparecerá la Lista de documentos recomendados.
2. Haga clic en Mostrar filtro.
3. Rellene los campos según sea necesario. Los siguientes campos necesitan una mayor explicación.

Tipo

Especifica un tipo de condición para buscar coincidencias en el documento y se lo presenta como un vínculo de documento recomendado.

Phrase/Keywords

Especifica información de consulta de búsqueda para identificar el concepto deseado contenido en el documento.

Haga clic en Buscar.

La lista Documentos recomendados se rellena con todos los elementos que coinciden con los criterios de búsqueda.

Configuración de los valores de búsqueda predeterminados

Puede configurar las opciones de búsqueda para que se utilicen como las opciones predeterminadas que aparecen cuando los usuarios buscan el conocimiento mediante el campo de búsqueda.

Nota: Estas opciones de búsqueda se sustituirán por los valores de búsqueda personales que los usuarios definan en la ventana Preferencias o por las opciones de búsqueda adicionales del panel Búsqueda de conocimiento de la ficha Conocimiento o del panel Categorías del conocimiento de la ficha Administración.

Procedimiento para configurar las opciones de búsqueda predeterminadas

1. En la ficha de Administración, vaya a Conocimiento, Buscar, Valores de búsqueda.

Aparecerá la página Opciones de búsqueda.

2. Seleccione las opciones siguientes, según corresponda:

Resultados recomendados

Especifica el número de documentos para mostrar en la lista de resultados de la búsqueda.

Campos de búsqueda predeterminados

Se especifican los campos de documento que se incluirán de forma predeterminada en las búsquedas por palabras clave. Active una casilla de verificación para incluir el campo asociado en las búsquedas predeterminadas. Desactive casilla de verificación para excluir el campo asociado de las búsquedas predeterminadas. Los siguientes campos de documento están disponibles para realizar las búsquedas:

- Título
- Resumen
- Problema
- Resolución
- Adjuntos

Configuración de búsqueda para todos los orígenes

Especifica si las búsquedas pueden incluir todos los orígenes de conocimiento. Por ejemplo, las categorías del conocimiento y las áreas de solicitud.

Configuración de búsqueda en un contexto de ticket

Especifica si las búsquedas pueden incluir todos los campos definidos en un ticket de centro de servicio al usuario (incidente, problema, incidencia, orden de cambio o solicitud).

- Para estas opciones, seleccione *uno* de los siguientes tipos de coincidencia:
 - **Cualquiera de las palabras (O):** Incluye un documento en el conjunto de resultados cuando contiene cualquiera de las palabras introducidas en el campo de búsqueda. Esta opción es la selección predeterminada.
 - **Todas las palabras (Y):** Incluye un documento en el conjunto de resultados sólo cuando contiene todas las palabras introducidas en el campo de búsqueda.

Haga clic en Guardar.

Se configuran los valores de búsqueda predeterminados.

Opciones de integración de CA Service Desk Manager

Las siguientes opciones de configuración están disponibles para la integración de CA Service Desk Manager:

Asignación de campos

Especifica los campos de CA Service Desk Manager que se deben rellenar con información de Gestión del conocimiento, y si se debe sobrescribir la información existente.

Configuración de búsqueda de incidencias

Selecciona los campos de búsqueda al hacer clic en el botón Buscar conocimiento en un ticket.

Configuración de búsqueda de envío de solicitudes

Selecciona los campos de búsqueda al hacer clic en el botón Buscar en un ticket.

Configuración de búsqueda de solíc./inci./probl.

Selecciona los campos de búsqueda al hacer clic en el botón Buscar en un ticket.

Sugerir conocimiento

Selecciona los campos de búsqueda al hacer clic en el botón Visualizar conocimiento antes de guardar en un ticket.

Más información:

[Definición de asignación de campos](#) (en la página 899)

[Definición de la configuración de búsqueda de incidencias](#) (en la página 902)

[Definición de la configuración de búsqueda de solicitudes/incidentes/problemas](#) (en la página 903)

[Sugerencias de conocimiento](#) (en la página 904)

[Definición de categorías de incidencia](#) (en la página 904)

[Definición de áreas de solicitud/incidente/problema](#) (en la página 905)

[Configuración de políticas de autoservicio](#) (en la página 907)

Definición de asignación de campos

Los administradores pueden utilizar la página Asignación de campos para especificar los campos que se deben rellenar con información de Gestión del conocimiento y si se debe sobrescribir la información existente.

Procedimiento para definir campos en el centro de servicio al usuario para Gestión del conocimiento

1. En la ficha Administración, vaya a Conocimiento, Integración de Service Desk, Asignación de campos.

Aparecerá la página Asignación de campos.

2. Rellene los campos siguientes según sea necesario:

Rellenar los valores de Service Desk desde Gestión del conocimiento

Especifica si se debe utilizar la información de Gestión del conocimiento para rellenar los campos de las incidencias o solicitudes de Service Desk al usuario.

- Active la casilla de verificación para que los campos de las columnas Rellenar los valores de Service Desk vacíos y Sobrescribir valores de Service Desk de Gestión del conocimiento estén disponibles para que pueda especificar qué información de Gestión del conocimiento se debe utilizar para rellenar los campos de las incidencias o solicitudes de centro de servicio al usuario.
- Desactive la casilla de verificación para que no estén disponibles los campos Rellenar los valores de Service Desk vacíos y Sobrescribir valores de Service Desk de Gestión del conocimiento. En este caso, los usuarios deben rellenar manualmente las incidencias o solicitudes de centro de servicio al usuario creadas desde Gestión del conocimiento.

Valor predeterminado: esta casilla de verificación está activada.

Service Desk

Identifica los campos de las incidencias o solicitudes que se corresponden con los campos que aparecen en la columna de Gestión del conocimiento.

La incidencia o solicitud se rellenará con la información procedente de los campos de la columna de Gestión del conocimiento correspondientes a las casillas de verificación activadas en la columna Rellenar los valores de Service Desk vacíos.

Gestión del conocimiento

Identifica los campos de Gestión del conocimiento que corresponden a los campos del centro de servicio al usuario que aparecen en la columna de Service Desk.

La incidencia o solicitud se rellenará con la información procedente de los campos de la columna de Gestión del conocimiento correspondientes a las casillas de verificación activadas en la columna Rellenar los valores de Service Desk vacíos.

La columna Gestión del conocimiento contiene dos listas desplegables:

- La primera lista desplegable se corresponde con el campo Resumen de la columna Service Desk y especifica el campo de Gestión del conocimiento (Título, Resumen o Problema) con el que se debe rellenar el campo Resumen de una incidencia o solicitud.

Valor predeterminado: resumen.

- La segunda lista desplegable se corresponde con el campo Descripción de la columna Service Desk y especifica el campo de Gestión del conocimiento (Título, Resumen o Problema) con el que se debe rellenar el campo Descripción de una incidencia o solicitud.
- **Valor predeterminado:** problema.

Rellenar los valores de Service Desk vacíos

Especifica qué campos vacíos de una incidencia o solicitud de centro de servicio al usuario se deben rellenar con información de Gestión del conocimiento.

- Active una casilla de verificación para asignar información desde un campo de Gestión del conocimiento al campo correspondiente del centro de servicio al usuario si dicho campo no contiene actualmente información.
- Desactive una casilla de verificación si no desea asignar información desde el campo de Gestión del conocimiento al campo correspondiente del centro de servicio al usuario.

Valor predeterminado: las casillas de verificación que corresponden a los campos

Resumen, Descripción, Producto, Activo y Área de solicitud en el centro de servicio al usuario están activadas.

Sobrescribir valores de Service Desk

Especifica qué campos vacíos de una incidencia o solicitud de centro de servicio al usuario se deben sobrescribir con información de Gestión del conocimiento.

- Active una casilla de verificación para reemplazar la información del campo del centro de servicio al usuario con la información del campo correspondiente de Gestión del conocimiento.
- Desactive una casilla de verificación si no desea reemplazar la información del campo del centro de servicio al usuario con la información del campo correspondiente de Gestión del conocimiento.

Estas casillas de verificación sólo están disponibles cuando las correspondientes casillas de verificación de las columnas Rellenar valores de Service Desk vacíos están seleccionadas.

Valor predeterminado: ninguna casilla de verificación Sobrescribir valores de Service Desk está activada.

Haga clic en Guardar.

Se define la asignación de campos.

Definición de la configuración de búsqueda de incidencias

Puede definir los campos de una incidencia que se van a buscar al hacer clic en el botón Buscar conocimiento de un ticket. Los campos seleccionados se copian a los campos correspondientes del Filtro de búsqueda en la ficha Conocimiento de la ventana Detalle de incidencia. Los campos del filtro de búsqueda se rellenan con información del parte si se selecciona la ficha Conocimientos o se hace clic en el botón Restablecer filtro de esa misma ficha.

Procedimiento para definir los campos de una incidencia que se utilizan para realizar búsquedas en la base de conocimiento

1. En la ficha Administración, seleccione Conocimiento, Integración de CA Service Desk Manager, Configuración de búsqueda de incidencias.
Aparecerá la página Integración de CA Service Desk Manager.
2. Seleccione los campos que desea que estén disponibles para búsquedas de base de conocimiento.
 - Resumen
 - Descripción
 - Elemento de configuración
 - Prioridad
 - Categoría
 - Causa raíz
 - Producto

Nota: No se pueden seleccionar al mismo tiempo los campos Resumen y Descripción.
3. Seleccione la opción Ejecutar búsqueda de manera automática cuando se selecciona la ficha Conocimiento de una incidencia si desea realizar automáticamente una búsqueda en la base de conocimiento cuando la ficha Conocimiento de la página de detalle está seleccionada.
4. Haga clic en Guardar.
Se ha configurado la búsqueda de incidencias.

Definición de la configuración de búsqueda de solicitudes/incidentes/problemas

Puede definir los campos de una solicitud, un incidente o un problema que se van a buscar al hacer clic en el botón Buscar conocimiento de un ticket. Los campos seleccionados se copian a los campos correspondientes del Filtro de búsqueda en la ficha Conocimiento de la página de detalles del ticket. Los campos del filtro de búsqueda se rellenan con información del parte si se selecciona la ficha Conocimientos o se hace clic en el botón Restablecer filtro de esa misma ficha.

Procedimiento para definir los campos de una solicitud, un incidente o un problema que se utilizarán para realizar búsquedas en la base de conocimiento

1. En la ficha Administración, seleccione Conocimiento, Integración de CA Service Desk Manager, Configuración de búsqueda de solíc./inci./probl.
Aparecerá la página Integración de CA Service Desk Manager.
2. Seleccione los campos que desea que estén disponibles para búsquedas de base de conocimiento.

- Resumen
- Descripción
- Elemento de configuración
- Severidad
- Impacto
- Urgencia
- Prioridad
- Área de solicitud
- Causa raíz

Nota: No se pueden seleccionar al mismo tiempo los campos Resumen y Descripción.

3. Seleccione la opción Ejecutar búsqueda de manera automática cuando se selecciona la ficha Conocimiento de una solicitud si desea realizar automáticamente una búsqueda en la base de conocimiento cuando la ficha Conocimiento de la página de detalle está seleccionada.
4. Haga clic en Guardar.

Se han configurado los campos de una solicitud, un incidente o un problema que se utilizarán para realizar búsquedas en la base de conocimiento.

Sugerencias de conocimiento

Los empleados y clientes pueden, si se les permite, ver una lista de sugerencias de conocimiento cuando crean un ticket en la interfaz de autoservicio.

Cuando se encuentra una solución y no se guarda el ticket, los documentos sugeridos se pueden acreditar a través de un sistema de valoración de autoservicio en el formulario de documento. Este sistema de valoración difiere en función de la configuración de la política de autoservicio definida en la página Valores de búsqueda.

Los datos recuperados se pueden utilizar en informes, cuadros de mandos y también cuando se realizan búsquedas en la base de conocimiento, donde los usuarios pueden filtrar los documentos que han resuelto con éxito los tickets.

Los beneficios de autoservicio se constatan con una menor cantidad de llamadas de soporte y la creación de un gran número de tickets, que se traduce en una reducción de los costes de explotación.

El administrador debe habilitar esta opción antes del uso; y debe configurar las categorías de incidencia apropiadas y las áreas de solicitud en las que se sugiere conocimiento en la interfaz de autoservicio.

Definición de categorías de incidencia

Puede definir categorías de incidencia en las que se sugiere conocimiento a los clientes y empleados durante la creación de tickets.

También puede marcar la característica Sugerir conocimiento como activa o inactiva. Al marcar esta característica como inactiva, deja de estar disponible para los clientes y empleados, pero sigue estando disponible en la base de datos para su uso futuro. Si decide utilizar esta característica en el futuro, puede volver y marcarla como activa.

Procedimiento para definir categorías de incidencia sugerir conocimiento

1. En la ficha de Administración, vaya a Conocimiento, Integración de Service Desk, Sugerir conocimiento, Categorías de incidencia.
Aparecerá la página Sugerir conocimiento para las categ. de incidencias.
2. Seleccione la opción **No sugerir conocimiento** para marcar la característica Sugerir conocimiento como activa.

Valor predeterminado: inactiva

Si marca esta característica, aparecen las siguientes opciones:

El conocimiento predeterminado será:

Sugerido

Indica que *desea* que se sugiera conocimiento para todas las categorías de incidencia a excepción de las definiciones de la lista de categorías de incidencias.

No sugerido

Indica que *no desea* que se sugiera conocimiento para todas las categorías de incidencia a excepción de las definiciones de la lista de categorías de incidencias.

Para todas las áreas de solicitud, incidente o problema excepto para:

Muestra la lista de áreas de solicitud en la que se sugiere o no se sugiere conocimiento a los empleados y clientes en la interfaz de autoservicio. Al usuario de autoservicio no se le permite editar las áreas de solicitud; éstas son de sólo lectura.

3. Haga clic en *uno* de los siguientes botones:

Agregar

Agrega el área de solicitud seleccionada a la lista.

Quitar

Elimina de la lista el área de solicitud seleccionada.

Quitar todos

Elimina de la lista todas las áreas de solicitud.

Guardar

Guarda la información de área de solicitud en la base de conocimiento.

Se han definido las categorías de incidencia.

Definición de áreas de solicitud/incidente/problema

Puede definir las áreas de solicitud, problema e incidente para las que se sugiere conocimiento a los clientes y empleados durante la creación del ticket.

También puede marcar la característica Sugerir conocimiento como activa o inactiva. Al marcar esta característica como inactiva, deja de estar disponible para los clientes y empleados, pero sigue estando disponible en la base de datos para su uso futuro. Si decide utilizar esta característica en el futuro, puede volver y marcarla como activa.

Procedimiento para definir las áreas de solicitud/incidente/problema para sugerir conocimiento

1. En la ficha Administración, vaya a Conocimiento, Integración de CA Service Desk Manager, Sugerir conocimiento, Áreas de solicitud/incidente/problema.

Aparecerá la página Sugerir conocimiento para áreas de solicitud/incidente/problema.

2. Seleccione la opción **No sugerir conocimiento** para marcar la característica Sugerir conocimiento como activa.

Valor predeterminado: inactiva

Si marca esta característica como activa, aparecen algunas opciones adicionales:

El conocimiento predeterminado será:

Sugerido

Especifique esta opción si desea que se sugiera conocimiento en todas las áreas de solicitud/incidente/problema excepto en aquellas definidas en la lista Área de solicitud.

No sugerido

Especifique esta opción si *no* desea que se sugiera conocimiento en todas las áreas de solicitud/incidente/problema excepto en aquellas definidas en la lista Área de solicitud.

Para todas las áreas de solicitud/incidente/problema excepto las indicadas:

Muestra la lista de áreas de solicitud en la que se sugiere o no se sugiere conocimiento a los empleados y clientes en la interfaz de autoservicio. Al usuario de autoservicio no se le permite editar las áreas de solicitud; éstas son de sólo lectura.

3. Haga clic en *uno* de los siguientes botones:

Agregar

Agrega el área de solicitud seleccionada a la lista.

Quitar

Elimina de la lista el área de solicitud seleccionada.

Quitar todos

Elimina de la lista todas las áreas de solicitud.

Guardar

Guarda la información de área de solicitud en la base de conocimiento.

Se han definido las áreas de solicitud/incidente/problema para sugerir conocimiento.

Configuración de políticas de autoservicio

Puede configurar políticas de autoservicio que acrediten documentos en función de un conjunto de escenarios de usuario.

Procedimiento para configurar políticas de autoservicio

1. En la ficha Administración, vaya a Conocimiento, Integración de CA Service Desk Manager, Sugerir conocimiento, Configuración de autoservicio.

Aparece la página Valores de búsqueda.
2. Especifique la configuración de política apropiada que acredite los documentos y guarde los tickets evitados en función de los siguientes escenarios de usuario:
 - El usuario no abrió ningún documento sugerido
 - El usuario abrió un documento sugerido
 - El usuario aceptó un documento sugerido como una solución a su problema
 - El usuario buscó conocimiento, abrió el documento y salió

Haga clic en Guardar.

Se ha guardado la configuración de la política de autoservicio.

Solution Survey

Las encuestas de soluciones permiten recopilar y analizar la opinión de los clientes sobre el rendimiento del documento de conocimiento. Puede modificar la configuración de la encuesta si selecciona Conocimiento, Encuesta de soluciones en la interfaz de administración. La encuesta aparece en un documento de conocimiento publicado, en el que los clientes, invitados y empleados pueden evaluar la eficacia del documento de conocimiento.

Esta característica contiene los siguientes componentes:

- Valores de FAQ
- Valores de estudio

Más información:

[Definición de valores de preguntas frecuentes](#) (en la página 908)

[Definición de los valores de la encuesta de soluciones](#) (en la página 910)

Definición de valores de preguntas frecuentes

Utilice la página Valores de preguntas frecuentes para definir los parámetros para los que el producto calcula la clasificación de preguntas frecuentes asignada a cada documento. El producto basa la clasificación de preguntas frecuentes en los siguientes criterios:

- La frecuencia con la que se ha accedido al documento anteriormente
- Lo útil que han encontrado los usuarios el documento
- Cómo ha disminuido la eficacia del documento con el paso del tiempo

De forma predeterminada, en la página de lista de documentos se muestran los documentos ordenados según la clasificación de preguntas frecuentes (es decir, en función de su utilidad). Los documentos más útiles "ascienden" a la parte superior de la lista de documentos. Con el tiempo, los documentos tienden a descender en la lista de documentos conforme los usuarios descubren soluciones a los problemas.

Procedimiento para definir los valores de preguntas frecuentes

1. Seleccione Conocimiento, Encuesta de soluciones, Valores de preguntas frecuentes en la ficha Administración.

Aparecerá la página Valores de preguntas frecuentes.

2. Rellene los campos siguientes según sea necesario:

Última modificación

Se especifica si se debe ejecutar el servicio de clasificación de preguntas frecuentes y se muestra la fecha en la que se actualizaron por última vez las clasificaciones de preguntas frecuentes.

- Active la casilla de verificación Ejecutar el servicio de clasificación de preguntas frecuentes para ejecutar el servicio de cálculo de preguntas frecuentes mediante los valores de esta ventana.
- Desactive la casilla de verificación Ejecutar el servicio de clasificación de preguntas frecuentes para que no se ejecute el servicio de cálculo de preguntas frecuentes.

Programación

Se define la frecuencia con la que el producto actualiza las clasificaciones de preguntas frecuentes. Este campo contiene los siguientes componentes:

Realizar el cálculo de preguntas frecuentes cada...

Especifica el tiempo que transcurre antes de que el producto actualice la clasificación de preguntas frecuentes de los documentos.

Valor predeterminado: 1 día

Desde...

Especifica la hora del día en la que el producto debe comenzar los nuevos cálculos de clasificaciones de preguntas frecuentes.

Valor predeterminado: 00:00 (12:00 A.M.)

Hasta...

Especifica la hora del día en la que el producto debe detener los nuevos cálculos de clasificaciones de preguntas frecuentes, independientemente si el cálculo ha terminado.

Valor predeterminado: 07:00 (7:00 A.M.)

Nota: Este valor se aplica por primera vez el día posterior a la instalación del producto. Por ejemplo, si instala el producto el 19 de abril de 2008, el servidor de preguntas frecuentes se ejecuta por primera vez el 20 de abril de 2008.

Antigüedad

Define el número de veces que se recalcula una clasificación de preguntas frecuentes del documento antes de que alcance 0. Según el valor especificado, la clasificación de preguntas frecuentes del documento se reduce y finalmente se convierte en 0, momento en el que aparece al final de la lista de documentos (cuando la lista se ordena por la clasificación de preguntas frecuentes).

Valor predeterminado: 180

Por ejemplo, si el valor Antigüedad es 180 en un documento con una clasificación de 4 (muy útil), la clasificación de preguntas frecuentes del documento será 0 cuando el producto vuelva a calcular la clasificación de preguntas frecuentes 180 veces.

Nota: De forma predeterminada, los cálculos de Bubble Up de preguntas frecuentes requieren datos bu_trans de los últimos 180 días, donde 180 es el factor de antigüedad. De esta forma, si cambia el factor de antigüedad de las preguntas frecuentes para que sea superior a 365 días, debe prolongar también las reglas de almacenamiento de la tabla bu_trans.

Días como nuevo

Especifica el número de días que un documento recién creado o importado se muestra en la carpeta Nuevos documentos de la ficha Conocimientos.

Valor predeterminado: 5 días

Clasificación

Especifica la clasificación predeterminada (Nada útil, Algo útil o Muy útil) de los documentos que los usuarios han abierto pero no clasificado.

Valor predeterminado: Algo útil

Haga clic en Guardar.

Se han definido los valores de preguntas frecuentes.

Definición de los valores de la encuesta de soluciones

Utilice la página Valores de la encuesta para configurar cómo se muestra un documento de conocimiento cuando se accede a éste para resolver un problema o contestar a una pregunta.

Procedimiento para definir los valores de la encuesta de soluciones

1. Seleccione Conocimiento, Encuesta de soluciones, Valores de la encuesta en la ficha Administración.

Aparecerá la página Valores de la encuesta.

2. Rellene los siguientes campos según sea necesario. Haga clic en Guardar.

Se han definido los valores de la encuesta de soluciones.

Configuración del sistema de Gestión del conocimiento

Puede definir la información predeterminada que se va a mostrar en la ficha Conocimiento en el inicio de sesión, el formato en el que las categorías se muestran en el panel Categorías del conocimiento de la ficha Administración y el número de documentos que se van a mostrar en la lista Mejores soluciones de la página principal de Gestión del conocimiento.

Más información:

[Configuración de los valores generales](#) (en la página 911)

Configuración de los valores generales

Puede definir la información predeterminada que se va a mostrar en la ficha Conocimiento en el inicio de sesión, el formato en el que las categorías se muestran en el panel Categorías del conocimiento de la ficha Administración y el número de documentos que se van a mostrar en la lista Mejores soluciones de la página principal de Gestión del conocimiento.

Para configurar los valores generales

1. Seleccione Administración, Conocimientos, Sistema, Valores generales en el panel izquierdo de la ficha Administración.
Aparece la página Valores generales.
2. Rellene los campos siguientes según sea necesario:

Pantalla de apertura de herramienta de búsqueda

Se especifica la información que se muestra de forma predeterminada en la ficha Conocimientos. Puede seleccionar una de las siguientes opciones:

- **Abrir con Preguntas frecuentes/Búsqueda:** Muestra los paneles Categoría, Búsqueda de conocimiento y Lista de documentos de conocimiento.
- **Abrir con ID de documento de árbol de conocimiento:** Muestra el árbol de conocimiento con el ID del documento especificado en el campo proporcionado. Puede volver al propio documento de árbol de conocimientos y, a continuación, a los paneles Categoría, Búsqueda de conocimientos y Lista de documentos de conocimientos.

Valor predeterminado: Abrir con Preguntas frecuentes/Búsqueda

Visualización de categorías

Se especifica el formato en el que se muestran las categorías de documento en el panel Categorías de conocimientos de la ficha Administración. Puede seleccionar una de las siguientes opciones:

- **Mostrar categorías en vista de árbol:** presenta las categorías en una estructura de árbol jerárquica en el panel Categorías de conocimiento. Las categorías se expanden y muestran las subcategorías asociadas. De esta forma, puede ver todas las categorías del árbol a la vez.
- **Mostrar categorías en vista de lista:** presenta las categorías en un formato de lista en el panel Categorías de conocimiento. Al seleccionar una categoría, sus subcategorías se muestran en una lista. Sólo puede ver el nivel actual de categoría o subcategorías en cada momento. Utilice el vínculo Subir un nivel para volver al nivel de categoría anterior.

Nota: Si tiene más de 250 categorías bajo la categoría superior, o bajo cualquier categoría, utilice la opción Mostrar categorías en vista de lista y no la vista de árbol.

Mejores soluciones

Especifica el número de documentos que se deben mostrar en la lista Mejores soluciones de la página principal de CA Service Desk Manager.

Valor predeterminado: 10

Incluir datos globales

Muestra los datos de todos los clientes en Mejores soluciones.

Valor predeterminado: activado

Notificaciones de indización de documentos

Define un usuario que debe recibir notificaciones por correo electrónico sobre el estado de la indización de documentos o cuando se producen errores en ésta. El usuario debe disponer de una dirección de correo electrónico en la tabla ca_contacts para poder recibir estas notificaciones. Utiliza la página Notificación del registro de contacto del asignatario para definir los métodos de notificación.

Importante: es muy importante que defina un asignatario para recibir notificaciones de indización de documentos en la sección Notificaciones de indización de documentos. Se debe definir una dirección de correo electrónico para este asignatario en la página Notificación de contactos para activar las notificaciones por correo electrónico.

Haga clic en OK.

Se han configurado los valores generales.

Capítulo 21: Administración de Automatización de soporte

Esta sección contiene los siguientes temas:

[Automatización el soporte en el entorno](#) (en la página 913)

[Administración del analista de Automatización de soporte](#) (en la página 916)

[Administración de usuarios de Automatización de soporte](#) (en la página 922)

[Administración de notificación de actividades de Automatización de soporte](#) (en la página 927)

[Adaptaciones de página de Automatización de soporte](#) (en la página 928)

[Propiedades del sistema de Automatización de soporte](#) (en la página 931)

[Administración de colas de Automatización de soporte](#) (en la página 931)

[Gestión de plantillas de tickets](#) (en la página 934)

[Valores de administración](#) (en la página 934)

[Cómo personalizar las herramientas de Automatización de soporte](#) (en la página 936)

[Administración del registro de sesión](#) (en la página 944)

[Informes de Automatización de soporte](#) (en la página 945)

Automatización el soporte en el entorno

Es posible implementar una estrategia de soporte mediante una combinación de procesos y herramientas. CA Service Desk Manager proporciona las herramientas para administrar la asistencia en vivo, desarrollar tareas automatizadas, y entregarlas a través de los diferentes canales de soporte.

Los procesos asociados se pueden utilizar para crear y mantener un entorno que realice lo siguiente:

- Reducir la duración media de la llamada de soporte
- Reducir los costes de soporte generales
- Aumentar las tasas de resolución
- Proporcionar una mayor satisfacción del usuario final

Asistencia en vivo

La asistencia en vivo proporciona el soporte de usuario final a través del uso de herramientas que mejoran la interacción remota entre analistas y usuarios finales. Puede utilizar respuestas predefinidas automatizadas, para comunicarse con el usuario final. Recopila información detallada sobre un equipo del usuario final, e interviene para proporcionar soporte.

Proporciona asistencia en vivo mediante las siguientes interfaces:

Interfaz de analista de Automatización de soporte

Permite a los analistas interactuar con los usuarios finales y brindar soporte durante sesiones de asistencia.

Cliente de End-User

Permite al usuario final charlar con el analista, mientras éste último realiza el soporte en el equipo del usuario.

Conectividad de Automatización de soporte

El analista y usuario final nunca se comunican directamente entre sí. No se necesita una conectividad de punto a punto directa entre los dos usuarios. Toda la transferencia de datos se dirige a través del servidor, verificando que la comunicación sea posible incluso cuando los equipos de los usuarios finales se encuentran detrás de cortafuegos restrictivos.

Puede conectar los equipos de los usuarios finales mediante las siguientes conexiones:

Socket

Utilizar una conexión de socket es la mejor manera de conectarse. Las conexiones de socket son el tipo de conexión más rápida y eficaz, que cuentan con la menor sobrecarga y una latencia mínima.

HTTP (o HTTPS)

El uso de una conexión HTTP puede dar lugar a mejores conexiones que una conexión de socket directa, debido a que los cortafuegos corporativos pueden bloquear estas últimas. Las conexiones HTTP generan una cantidad significativa de tráfico de red en comparación con las conexiones de socket directas. Debido a la sobrecarga HTTP y al procesamiento en el servidor, cuando la mayoría de las conexiones al servidor se realizan sobre HTTP, el número de sesiones simultáneas es mucho menor.

Proxy

El proxy de socket es un modo de operación del servidor de Automatización de soporte que se utiliza para descargar algunas de las operaciones de uso intensivo de CPU. Por ejemplo, el cifrado/descifrado del servidor principal, y proporcionar un componente de servidor que pueda atravesar la zona desmilitarizada (DMZ) o una zona similar de la topología de red lógica.

Típicamente se intenta, en primer lugar, establecer una conexión de socket directa y, a continuación, conectarse a través de HTTP si ésta falla. Sin embargo, puede especificar configuraciones de conexión personalizadas en el equipo cliente para alterar esta secuencia.

Nota: Para obtener más detalles sobre la configuración de comunicaciones, consulte la *Ayuda en línea*.

Cliente de usuario final

El cliente de usuario final conecta los usuarios finales con los analistas en las sesiones de asistencia en vivo. Los usuarios finales charlan con los analistas en una conversación Web, pero si deben utilizar las herramientas en la interfaz de analista de Automatización de soporte, CA Service Desk Manager inicia el cliente en el equipo de usuario final.

Carga de servidor

En grandes implementaciones, una carga de servidor alta puede degradar el rendimiento de la aplicación. Por este motivo, se puede transferir una parte del procesamiento a uno o varios servidores proxy de sockets, de la siguiente manera:

- Transferir el cifrado y descifrado de los datos entrantes y salientes de todos los analistas o clientes (conectándolos a través de proxy directo o HTTP).
- Transferir el procesamiento del tráfico HTTP desde y hacia aquellos clientes que se conectan a HTTP a través del proxy de socket.

Componente del servidor en la DMZ

En ciertos entornos de red, permitir el acceso de socket directo a los servidores de aplicaciones que ejecutan la aplicación de servidor de Automatización de soporte, se puede considerar un riesgo de seguridad. En estos entornos, puede utilizar el proxy de sockets dentro de la DMZ para proporcionar un componente intermediario entre los usuarios de Internet y los servidores de aplicaciones. En este escenario, el uso del proxy de socket descarga una parte del procesamiento del servidor primario.

Cómo funciona un proxy de socket

El proxy de socket funciona de la siguiente manera:

1. En el puerto externo configurado, el proxy de socket escucha las conexiones entrantes de los analistas o usuarios finales.
2. El proxy de socket establece una conexión punto a punto con el servidor primario en el puerto interno configurado, para cada conexión. Estas dos conexiones se denominan conexión de usuario final y conexión de servidor, respectivamente.
3. Las conexiones de usuario final están cifradas y el proxy de socket cifra o descifra los datos que entran o salen de la conexión de usuario final.

Nota: Las conexiones del servidor no están cifradas.

4. En cada paquete de datos entrante, se verifica la estructura de protocolo y se valida un valor de suma de comprobación antes de pasar los datos al servidor primario mediante la conexión de servidor.
5. El servidor primario transfiere el procesamiento de cifrado y descifrado.
6. El proxy de socket cierra la conexión punto a punto correspondiente una vez que se cierra la conexión de usuario final o de servidor.

Administración del analista de Automatización de soporte

Los analistas de Automatización de soporte controlan y gestionan varias solicitudes de usuario final en sesiones de asistencia en vivo en el entorno. Los analistas utilizan herramientas de Automatización de soporte para interactuar con los usuarios finales y proporcionar asistencia en vivo.

Los analistas acceden a la interfaz desde un ticket de CA Service Desk Manager, por ejemplo un incidente, o desde la ficha de Automatización de soporte. Puede gestionar niveles de acceso para establecer permisos para las herramientas que pueden utilizar los analistas. Puede habilitar y deshabilitar las herramientas de Automatización de soporte para clientes específicos. Si la herramienta se deshabilita para un cliente, los analistas no podrán utilizarla en las sesiones de asistencia.

Importante: la interfaz de analista de Automatización de soporte sólo se ejecuta en Windows. Para obtener más información sobre los sistemas operativos soportados, consulte las *Notas de la versión*.

Más información:

[Modo en el que los analistas inician la asistencia en vivo](#) (en la página 917)

[Cómo configurar la asistencia en vivo para analistas](#) (en la página 919)

[Modo en el que los usuarios finales se unen a las sesiones de asistencia](#) (en la página 920)

[Modo en el que los analistas automatizan el soporte para los usuarios finales](#) (en la página 921)

[Modo en el que los analistas proporcionan la asistencia en vivo](#) (en la página 921)

Modo en el que los analistas inician la asistencia en vivo

Los analistas inician la asistencia en vivo como sigue:

1. El analista realiza *cualquiera* de las siguientes acciones:
 - Inicia sesión en CA Service Desk Manager y selecciona la ficha Automatización de soporte.
 - Abre un ticket de CA Service Desk Manager y selecciona la ficha Automatización de soporte.
2. CA Service Desk Manager solicita al analista la instalación de la versión 1.6 o posterior de Java Runtime Environment (JRE), si aún no está instalada.
CA Service Desk Manager inicia la interfaz de analista de automatización de soporte.

Nota: La tabla sa_login_session crea un registro cada vez que un analista inicia la interfaz de analista de automatización de soporte y cuando un usuario final inicia el cliente Web. Para obtener más información sobre la tabla sa_login_session, consulte la *Guía de referencia técnica de CA Service Desk Manager*.

Configuración de opciones de conexión de Java

Puede configurar opciones de conexión de Java para resolver una incidencia en la que la interfaz de analista de Automatización de soporte no puede conectarse al servidor de Automatización de soporte. Esta incidencia se produce cuando la configuración predeterminada del explorador del analista no se ha configurado adecuadamente y presenta errores al iniciar la asistencia en vivo. Puede editar la configuración de la conexión del analista en un explorador o en el panel de control de Java.

Procedimiento para configurar las opciones de conexión en el explorador

1. Abra el explorador Web, por ejemplo Internet Explorer.
Aparece el explorador.
2. Seleccione Herramientas, Opciones de Internet.
Aparecerá el cuadro de diálogo Opciones de Internet.
3. Configure la configuración de conexión que corresponda, por ejemplo una conexión directa o un servidor proxy.
4. Haga clic en OK.
Se configuran las aperturas de conexión.

Procedimiento para configurar las opciones de conexión en el panel de control de Java

1. Abra el panel de control de Java con el siguiente comando:
`javaws -viewer`
Aparece la ventana Panel de control de Java.
2. En la ficha General, haga clic en Configuración de Red.
Aparecerá el cuadro de diálogo Configuración de Red.
3. Configure los valores apropiados, por ejemplo una conexión directa o un servidor proxy.
Haga clic en OK.
Se configuran las aperturas de conexión.

Cómo configurar la asistencia en vivo para analistas

La interfaz de analista de automatización de soporte se configura estableciendo el rol y los permisos de seguridad para los analistas en el entorno de asistencia en vivo, de la siguiente manera:

1. Creación o modificación de roles (see page 923) y niveles de acceso de Automatización de soporte (see page 926) apropiados para los analistas en el entorno de asistencia en vivo.

Los roles y niveles de acceso se actualizan para conceder a los analistas permisos para herramientas específicas que pueden utilizar en las sesiones de asistencia.

2. Establecimiento y gestión de colas (see page 931) para el entorno de asistencia en vivo.

Las colas se crean para dirigir apropiadamente las solicitudes de asistencia en vivo entrantes.

3. Establecimiento y gestión de notificaciones de actividades (see page 927) para el entorno de asistencia en vivo.

Las notificaciones de correo electrónico se crean para alertar a los analistas cuando obtienen una solicitud de sesión de asistencia en la cola.

4. Establecimiento y gestión de conversaciones preestablecidas (see page 943) para el entorno de asistencia en vivo.

Se crean conversaciones preestablecidas que los analistas utilizan para enviar respuestas preconfiguradas a las preguntas más frecuentes y a situaciones comunes.

5. Establecimiento y gestión de tareas automatizadas para el entorno de asistencia en vivo.

Las tareas automatizadas se crean para ejecutar acciones específicas en el equipo del usuario final.

Nota: Los scripts sólo se pueden crear y cargar al servidor a través del IDE del editor de tareas automatizadas.

Modo en el que los usuarios finales se unen a las sesiones de asistencia

Un usuario final solicita sesiones de asistencia desde su página principal de CA Service Desk Manager o poniéndose directamente en contacto con la asistencia técnica, por ejemplo por teléfono o correo electrónico. El analista de Automatización de soporte invita al usuario final a una sesión desde el ticket de CA Service Desk Manager.

1. El usuario final realiza *cualquiera* de las siguientes acciones:

- Solicita una conversación en vivo desde la página principal de CA Service Desk Manager.

Aparece la página de inicio de conversación en vivo que solicita al usuario final el área y la descripción del incidente. El usuario final hace clic en Continuar, abre la sesión, y el usuario final se sitúa en la cola apropiada.

- Hace clic en un vínculo incluido en una notificación de correo electrónico y se conecta en la sesión de asistencia utilizando sus credenciales y un código de inicio de sesión proporcionado por el analista.

Si el usuario final inicia sesión desde la notificación de correo electrónico, omite la cola.

- Hace clic en Unirse ahora al analista y proporciona el código de inicio de sesión para omitir la cola.

Nota: Cuando se inicia el cliente de usuario final de Automatización de soporte, se descarga un archivo ejecutable para iniciar el programa. El usuario final lo inicia en forma manual aunque, por razones de seguridad, hay un tiempo limitado para iniciar el archivo ejecutable. Después de que el tiempo caduca, aparece un mensaje de error en el equipo del usuario final cuando se intenta iniciar el archivo ejecutable del lanzador.

2. El analista proporciona la asistencia en vivo al usuario final a través de la conversación. El usuario final utiliza su explorador Web para charlar con el analista, o puede iniciar la ejecución del agente.

Nota: Si el analista no puede resolver la sesión mediante WebChat, en la ventana Sesión de analista puede invitar al usuario final a utilizar las herramientas completas disponibles en la interfaz de analista de automatización de soporte. El usuario final debe aceptar la solicitud para iniciar el cliente en su equipo y para que el analista pueda utilizar estas herramientas.

Modo en el que los analistas automatizan el soporte para los usuarios finales

Los analistas utilizan las herramientas de asistencia en vivo para ejecutar las siguientes tareas en los equipos del usuario final:

- Sesiones de chat en vivo de host
- Visualización de sistemas de archivos
 - Creación, modificación, cambio de nombre o supresión de archivos y directorios
 - Copia y transferencia de archivos y carpetas al equipo del usuario final
- Visualización de registros del sistema
 - Creación, edición o supresión de registros
 - Exportación o importación de valores de registro del registro del usuario final
- Captura de pantallas del usuario final cuando la calidad de conexión no es suficiente para proporcionar la asistencia por control remoto
- Visualización del escritorio del equipo del usuario final
- Control en forma remota del equipo del usuario final
- Inicio de un programa en el equipo del usuario final
- Reinicio o apagado del equipo del usuario final
- Ejecutar tareas automatizadas

Nota: Para obtener información detallada sobre el modo en el que los analistas utilizan las herramientas de asistencia en vivo, consulte la *Ayuda en línea*.

Más información:

[Administración de nivel de acceso de Automatización de soporte](#) (en la página 926)

Modo en el que los analistas proporcionan la asistencia en vivo

Los analistas proporcionan la asistencia en vivo a los usuarios finales mediante la interfaz de analista de automatización de soporte. Los analistas controlan los usuarios finales para dirigirlos a sus colas, gestionan sesiones de asistencia y se unen a las sesiones para las que tienen permiso.

1. El usuario final solicita una sesión de asistencia en la página principal de CA Service Desk Manager, o en un ticket, por ejemplo un ticket de incidente, solicitud o incidencia.

2. El usuario final se une a una cola.

Nota: Si el usuario final se une a la sesión utilizando el vínculo de la invitación de correo electrónico del analista, omite la cola.

Puede configurar las áreas de solicitud y las categorías de incidencia de CA Service Desk Manager para el enrutamiento de la cola.

3. El analista selecciona el usuario final en la cola.
4. La sesión de asistencia comienza y el analista proporciona la asistencia en vivo.

Nota: Si el analista inicia la interfaz de analista de automatización de soporte en la ficha Automatización de soporte, ningún ticket de CA Service Desk Manager está asociado con la sesión de asistencia.

5. El analista crea el ticket al cerrar la sesión de asistencia y define el estado como *Automatización de soporte: abierto* o *Automatización de soporte: abierto*, o transfieren la sesión de asistencia a otra cola.
6. El analista cierra la sesión y el usuario final recibe una notificación de correo electrónico con el registro de sesión.

Nota: Para obtener más detalles sobre cómo los analistas controlan las colas y gestionan las sesiones de asistencia, consulte la *Ayuda en línea*.

Administración de usuarios de Automatización de soporte

Los administradores del sistema y administradores de clientes configuran contactos, permisos de rol, niveles de acceso y niveles de privacidad de CA Service Desk Manager para definir los permisos de usuario. A continuación, se muestran los usuarios que utilizan Automatización de soporte.

Administrador del sistema

Define el acceso al sistema para agregar, editar y modificar todos los valores predeterminados y funciones de Automatización de soporte en la ficha Administración. El administrador del sistema define clientes y analistas, personaliza las propiedades del sistema de Automatización de soporte y ejecuta los restablecimientos de contraseñas del sistema.

Administrador de clientes

Define los derechos administrativos a nivel de cliente, pero no concede acceso para crear o editar otros clientes ni restablecer contraseñas de usuario. El cliente proveedor de servicios determina los permisos.

Analista

Define los derechos del usuario que proporciona asistencia en vivo a los usuarios finales en su entorno de soporte.

Usuario final

Define los derechos de los usuarios que pueden solicitar asistencia en vivo a los analistas en su entorno de soporte, como por ejemplo empleados y clientes.

Cómo configurar los permisos de rol de Automatización de soporte

Puede configurar roles de CA Service Desk Manager para disponer de permisos de Automatización de soporte. Puede establecer permisos de rol a través de la configuración de niveles de acceso de Automatización de soporte para los analistas y de niveles de privacidad para los usuarios finales en el entorno de asistencia en vivo, como se indica a continuación.

1. Configure los niveles de acceso para analistas adecuados en el entorno de asistencia en vivo.

Los niveles de acceso de analista se crean para gestionar los permisos de analista en el sistema, por ejemplo para habilitar y deshabilitar herramientas específicas de la interfaz de analista de Automatización de soporte.

2. Configure los niveles de privacidad para usuarios finales adecuados en el entorno de asistencia en vivo.

Los niveles de privacidad se crean para gestionar los niveles de acceso de usuario final en su sistema.

3. Asignación (see page 927) de niveles de acceso a roles.

Los niveles de privacidad del usuario final y los niveles de acceso del analista se asignan a roles del entorno.

Nota: Para obtener información detallada sobre cómo crear y modificar niveles de acceso de Automatización de soporte para los analistas y cómo configurar niveles de seguridad para los usuarios finales, consulte la *Ayuda en línea*.

Usuarios registrados y anónimos de Automatización de soporte

El servidor de Automatización de soporte acepta usuarios registrados o anónimos, en función de los permisos de CA Service Desk Manager. Si tiene el permiso para hacerlo, el usuario invitado permite que los usuarios anónimos inicien sesión en CA Service Desk Manager. Puede realizar la autenticación con el servidor para obtener acceso a los siguientes servicios:

- Asistencia en vivo
- Autoservicio
- Editor de tareas automatizadas
- Cliente de usuario final

Cómo configurar Automatización de soporte para los usuarios invitados

Puede configurar el entorno de asistencia en vivo para permitir usuarios invitados. Los usuarios invitados se configuran para clientes específicos o se los pone a disposición de todo el sistema, como se indica a continuación:

1. Crear un tipo de acceso que permita la autenticación Web (see page 924).

Se debe seleccionar el tipo de validación "Abierto - Permitir siempre el acceso" .

2. Asignar (see page 925) el tipo de acceso a un contacto.

Puede crear un contacto invitado para diferentes clientes de su entorno.

3. Notifique a los usuarios adecuados de su entorno acerca del inicio de sesión anónimo, mediante el siguiente formato de URL:

`http://nombre de host?USRNAME=Nombre de usuario`

Creación de un tipo de acceso para usuarios invitados

Puede crear un tipo de acceso que permita a los usuarios invitados iniciar sesión en CA Service Desk Manager sin autenticarse. El proveedor de servicios puede crear un tipo de acceso de invitado para cada cliente de su entorno.

Procedimiento para crear un tipo de acceso de invitado

1. Haga clic en Gestión de roles y seguridad, Tipos de Acceso.

Aparece la Lista de tipos de accesos.

2. Haga clic en Crear nuevo.

Aparecerá la página Crear nuevo tipo de acceso.

3. Complete los campos según corresponda, por ejemplo símbolo y descripción.
4. En la ficha Autenticación Web, seleccione *Abierto - Permitir siempre el acceso* de la lista desplegable Tipo de validación.
5. Guarde el tipo de acceso.
Se crea el tipo de acceso.
6. (Opcional) Haga clic con el botón secundario en la página de lista Tipo de acceso para actualizar la página de lista.
Aparece el tipo de acceso de invitado en la lista.

Asignación del tipo de acceso de invitado para un contacto.

Puede asignar el tipo de acceso de invitado a un contacto después de crear un tipo de acceso que utiliza autenticación Web para que el contacto pueda conectarse a CA Service Desk Manager. Puede notificar a los usuarios apropiados del entorno sobre el contacto de invitado después de asignarle el tipo de acceso.

Procedimiento para asignar el tipo de acceso de invitado

1. Haga clic en Gestión de roles y seguridad, Contactos.
Aparecerá la página Búsqueda de contactos.
2. Haga clic en Crear nuevo.
Aparecerá la página Crear nuevo contacto.
Nota: También puede modificar un contacto.
3. En la lista desplegable Tipo de contacto, seleccione invitado.
4. (Opcional) Asociar el contacto con un cliente. También se puede definir el contacto como público.
5. Guarde el contacto.
Se crea el contacto y se lo asocia el tipo de acceso de invitado.

Administración de nivel de acceso de Automatización de soporte

Puede gestionar los niveles de acceso de Automatización de soporte y asignarlos a roles de CA Service Desk Manager en el entorno de soporte. Los entornos de soporte varían en su tamaño y estructura, de modo que la implementación de los niveles de acceso también puede variar.

Un pequeño entorno de soporte puede tener solamente uno o dos analistas categorizados con un único nivel de acceso, como por ejemplo Analista. En un entorno de soporte mayor, el administrador de clientes puede configurar muchos niveles de acceso de analista, cada uno con privilegios de acceso y soporte diferentes.

Importante: En un entorno de multicitente, los analistas que no pertenecen al proveedor de servicios solamente tienen acceso de escritura a sus propios clientes y subclientes. Puede conceder el acceso de escritura de analista a otros clientes y subclientes si actualiza el acceso de función del cliente al que se tiene acceso, para incluir los clientes que no pertenecen al proveedor de servicio.

Están disponibles los siguientes niveles de acceso:

Analista

Especifica el tipo de contacto que proporciona asistencia en vivo a los usuarios finales en su entorno de soporte. Los niveles de acceso definen las colas, tareas automatizadas y herramientas que están a disposición del analista para su uso.

Usuario final

Especifica el tipo de contacto que recibe la asistencia en vivo de los analistas, por ejemplo empleado y cliente.

Puede gestionar los niveles de acceso de Automatización de soporte en la ficha Administración.

Nota: Para obtener información detallada sobre cómo crear y modificar niveles de acceso de Automatización de soporte para los analistas y usuarios finales, consulte la *Ayuda en línea*.

Asignar un nivel de acceso a un rol

Los niveles de acceso de Automatización de soporte se pueden asignar a los roles existentes de CA Service Desk Manager en el entorno.

Procedimiento para asignar un nivel de acceso a un rol

1. Seleccione Gestión de roles y seguridad, Gestión de roles, Lista de roles en la ficha Administración.

Aparecerá la página Lista de roles.

2. Haga clic en el rol al que desea asignar el nivel de acceso, por ejemplo Administrador.

Aparecerá la página Detalles del rol.

3. Haga clic en Editar.

Aparecerá la página Actualizar rol.

4. En la ficha Autorización, seleccione el nivel de acceso que ha creado en la lista desplegable del Acceso al servicio de automatización de soporte.

Aparecerá la página Detalles del rol. Verifique que el acceso de Automatización de soporte se asigna al rol.

Administración de notificación de actividades de Automatización de soporte

Las notificaciones de actividades sirven para gestionar las actividades de Automatización de soporte. Se puede personalizar el modo en el que los usuarios finales, analistas y administradores reciben las notificaciones cuando se produce una actividad, como por ejemplo el final de una sesión de asistencia.

Configure cualquiera de las notificaciones predeterminadas siguientes, de la manera más adecuada para su entorno:

Notificación de entrada de cola

Notifica al analista cuando un usuario final se une a una cola de sesión de asistencia.

Notifica al analista cuando la sesión de asistencia se transfiere a otra cola.

Notificación de analista

Notifica al analista cuando caduca el tiempo de espera de la cola de usuario final. El evento de caducidad se reconoce con una macro condicional de eventos de CA Service Desk Manager.

Invitación de usuario final a una sesión de asistencia - Incidente

Notifica al usuario final cuando el analista lo invita a una sesión de asistencia de un incidente o una solicitud.

Invitación de usuario final a una sesión de asistencia - Incidencia

Notifica al usuario final cuando el analista lo invita a una sesión de asistencia de una incidencia.

Notificación de fin de sesión

Notifica al sistema cuando finaliza la sesión de asistencia.

Importante: Si desea utilizar la funcionalidad de Automatización de soporte con un sistema externo como Star, el contacto `System_SA_User` se establece en la regla *Notificación de fin de sesión* de forma predeterminada.

Adaptaciones de página de Automatización de soporte

Se puede configurar el aspecto de las páginas de Automatización de soporte para los usuarios finales según las necesidades empresariales. Las siguientes adaptaciones le permiten controlar lo que el usuario visualiza antes de unirse a la sesión de asistencia y después de que la sesión se completa:

- Personalizar el encabezado y el pie de página de todas las páginas que visualiza el usuario final.

Puede cambiar código HTML del encabezado y pie de página y modificar la ubicación del archivo CSS que contiene las definiciones de estilos.
- Personalizar las necesidades de localización del entorno.

Se puede establecer la configuración local predeterminada para todos los analistas y usuarios finales.
- Personalizar los diseños de página que los usuarios finales visualizan cuando se conectan y esperan unirse a las sesiones de asistencia.

Puede personalizar las páginas dirigidas a los usuarios finales para adaptarlas a las necesidades del negocio.

Nota: Para obtener más detalles sobre la configuración de páginas de Automatización de soporte para analistas y usuarios finales, consulte la *Ayuda en línea*.

Administración de personalizaciones

Puede personalizar el encabezado y pie de página de las páginas visibles para el usuario final, por ejemplo la página de autoservicio. Puede cambiar el código HTML del encabezado y pie de página y modificar la ubicación del archivo CSS que contiene las definiciones de estilos.

Puede ver una lista de registros de personalización, una por cada cliente como máximo. Los clientes pueden crear sus propias personalizaciones, o utilizar la configuración del sistema predeterminada si no se ha definido una personalización para el cliente. También puede habilitar la localización de la personalización y ver una lista de todas las personalizaciones localizadas para las localizaciones habilitadas.

Importante: las marcas personalizadas de Automatización de soporte de CA r6.0 SR1 eFix5 no migran a CA Service Desk Manager r12.5 automáticamente. Recomendamos que revise la marca personalizada para verificar que corresponda a la marca de CA Service Desk Manager. Si es necesario, copie y pegue el encabezado, pie de página y datos de la URL de CSS de cada división al cliente (o público) correspondiente en CA Service Desk Manager para migrar los datos de personalizaciones.

Administración de localización

La localización permite admitir varios idiomas de manera simultánea en la misma instalación, mediante la traducción de los elementos de la aplicación a un idioma determinado. Estos elementos pueden incluir mensajes del sistema, iconos y contenido. La información se presenta de la mejor manera posible al usuario final, sin importar su idioma nativo.

Las versiones localizadas de Automatización de soporte cubren las necesidades del entorno global. Cada cliente puede administrar varios idiomas, y las localizaciones se admiten en varios clientes. Cada cliente comparte la configuración del sistema predeterminada con su localización. En la lista de mensajes habilitados, se puede configurar el idioma utilizado por el usuario final y el analista antes de iniciar la asistencia en vivo. En una sesión de asistencia, el analista puede utilizar un idioma diferente que el usuario final.

Puede editar el texto localizado para las cláusulas de exención de responsabilidad. No puede crear o quitar localizaciones, pero las puede habilitar o deshabilitar.

Nota: La interfaz de administrador solamente está disponible en la localización de servidor predeterminada.

Configuración de diseño de página

Cuando los usuarios finales se conectan a la asistencia en vivo desde CA Service Desk Manager, visualizan una página de inicio predeterminada. Asimismo, cuándo durante el inicio se los ubica en una cola, en espera, nuevamente ven una página predeterminada.

Si no se especifica ninguna configuración especial para los clientes, de forma predeterminada reciben la configuración pública. Puede configurar la configuración pública siguiente para las colas que no tienen configuraciones especializadas:

- Página de espera
- Página tras inicio de sesión del usuario final
- En sesión
- Página tras cierre de sesión
- Salir de la página Encuesta

Cada página incluye su propia página de detalles que está compuesta por un campo de texto para escribir la URL y una casilla de verificación para marcar esta página como externa.

Propiedades del sistema de Automatización de soporte

Puede personalizar muchas de las formas en las cuales Automatización de soporte controla las actividades para diferir de la instalación predeterminada. Puede utilizar los valores de configuración de las opciones predeterminadas del sistema para personalizar el comportamiento de Automatización de soporte. Por ejemplo, puede personalizar algunas de las opciones de Automatización de soporte siguientes:

- Habilitar o deshabilitar el vínculo para la conversación en vivo en la página principal de empleados y clientes de CA Service Desk Manager.
- Habilitar o deshabilitar el vínculo para unirse a una sesión en la página principal de empleados y clientes de CA Service Desk Manager.
- Habilite o deshabilite la opción de crear un incidente de CA Service Desk Manager cuando el usuario final se desconecta mientras espera que se lo atienda en una cola de Automatización de soporte.

Las propiedades del sistema son opcionales de cliente. Si un cliente no ha definido sus propiedades, Automatización de soporte utiliza los valores públicos (compartidos). La instalación del producto crea las propiedades públicas predeterminadas.

Nota: Para obtener más información acerca de la configuración de propiedades del sistema de Automatización de soporte, consulte la *Ayuda en línea*.

Administración de colas de Automatización de soporte

Las colas se pueden utilizar para dirigir las solicitudes de sesión de asistencia al analista más apropiado. El usuario final puede seleccionar una categoría, o escribir una descripción del problema del equipo, y su ticket (por ejemplo un incidente) se dirige a la cola apropiada.

Después de la instalación del producto inicial, la cola predeterminada se denomina Soporte. Se pueden definir varias colas para facilitar la clasificación y el seguimiento de las distintas solicitudes de soporte, según las necesidades empresariales. Sólo se puede asignar una cola predeterminada por cliente. Si no asigna el valor predeterminado a una cola de cliente, o si la cola de cliente predeterminada no está disponible, el sistema utiliza la cola predeterminada pública. Se deben definir las horas de trabajo por cola.

El sistema automáticamente determina dónde ubicar el usuario final. Para ello, asigna las colas en áreas de incidentes. Si un área se asigna a una cola, el usuario final selecciona una categoría y el sistema lo dirige a la cola apropiada. Las capacidades de búsqueda de FAST ESP se aplican a la descripción de un incidente o una categoría de incidencia a fin de identificar las colas relevantes, y el usuario final sólo se dirige a la cola que se ajusta en mayor medida.

Importante: Sólo se dispone de estas capacidades de búsqueda cuando se instala FAST ESP. Nota: Para obtener información sobre la instalación y configuración de FAST ESP, consulte la *Guía de implementación*.

Nota: Para obtener información detallada sobre personalización y asignación de colas de Automatización de soporte, consulte la *Ayuda en línea*.

Gestión de colas

Las colas se configuran para ayudar a los usuarios finales a recibir la asistencia en vivo apropiada de los analistas. Puede gestionar las colas se para mejorar el modo en el que los usuarios finales son dirigidos a las sesiones de asistencia, mediante las acciones siguientes:

- Personalizar las colas para los analistas y clientes del entorno de asistencia en vivo.

Puede activar o desactivar las colas y especificar permisos de clientes y analistas.

- Asignar una cola predeterminada.

Puede dirigir usuarios finales a la cola predeterminada cuando introducen consultas que no coinciden con las colas configuradas en el entorno. También puede personalizar las colas para los clientes de su entorno.

Nota: En caso de que falte la cola de cliente predeterminada o no esté disponible, se utilizará la cola pública.

- Asignar horas de operación para las colas.

Puede gestionar colas según la disponibilidad de los usuarios en su entorno de soporte, como por ejemplo la habilitación de los servicios de Automatización de soporte durante el horario laboral.

Importante: Puede asignar turnos tanto a las horas de Automatización de soporte como a colas individuales de asistencia en vivo. Los diferentes turnos que se asignan a colas individuales y horas de Automatización de soporte pueden causar conflictos a los analistas y usuarios finales en su entorno de soporte.

Cómo gestionar resúmenes de cola

Puede componer los campos que un analista visualiza en la página Resúmenes de cola. En el resumen de cola, no puede crear campos, pero puede realizar una selección del conjunto de campos siguientes:

- Cola
- Pregunta
- Tiempo de espera
- Correo electrónico
- Empresa
- Dirección IP
- Analista de propiedad
- Categoría
- Idioma
- Cliente

Cómo gestionar las horas de la cola

Puede habilitar Automatización de soporte para cada cola para horas del día específicas, para adaptar las horas de trabajo de los analistas de la siguiente manera:

- Cree una programación independiente para cada cola y para todos los servicios de soporte automatizados.

Nota: Estos valores no limitan las funciones de autoservicio.

- Defina las horas de soporte del servidor mediante un estado abierto o cerrado global. Una entrada para cada hora de la semana indica una diferencia con el estado global del servidor.
- El servidor utiliza la primera entrada de cada hora según las reglas que se hayan establecido.

Esta acción combina de manera eficaz las definiciones de las horas de soporte con los valores del cliente principal (o público). Esta acción puede tener resultados inesperados si se utiliza una mezcla de predeterminado-cerrado y predeterminado-abierto en la jerarquía.

Gestión de plantillas de tickets

Puede especificar qué plantillas de tickets están disponibles para la interfaz de usuario de analista. Puede seleccionar las plantillas de ticket para los tipos de ticket de incidencia e incidente/solicitudes.

Puede definir si la plantilla es predeterminada o activa. Cuando cree una plantilla de ticket, puede seleccionar entre las plantillas de CA Service Desk Manager existentes. La plantilla predeterminada debe estar activa.

Puede tener solamente una plantilla de ticket como predeterminada por cliente.

Nota: Si desea obtener información detallada sobre la personalización de plantillas de tickets, consulte la *Ayuda en línea*.

Valores de administración

Puede definir y configurar los siguientes valores de Automatización de soporte:

- Servidores de enrutamiento de mensajes
- Permisos de usuarios finales (Niveles de privacidad)
- Horas de Automatización de soporte

Cómo configurar los valores de Automatización de soporte

Puede configurar los valores de Automatización de soporte para el entorno de soporte según las necesidades empresariales. Los valores le permiten controlar la funcionalidad administrativa, como por ejemplo los servidores de enrutamiento de mensajes, los niveles de privacidad y las horas de Automatización de soporte.

- Configurar los servidores de enrutamiento de mensajes para mejorar el rendimiento durante la sesión de asistencia.

Puede conectar los usuarios finales al servidor local preferido del analista, o si la conexión no se puede realizar, conectar la sesión al servidor principal predeterminado.

- Definir los niveles de privacidad para los usuarios finales en el entorno.
Puede habilitar herramientas específicas de la interfaz de analista de Automatización de soporte, en función de los niveles de privacidad que se utilizan en el entorno.
- Establecer las horas de Automatización de soporte en horas específicas de operación o como abiertas en todo momento.
Puede dirigir las solicitudes de asistencia en vivo en el momento en que el centro de soporte permanece cerrado, como por ejemplo abrir una página de Web que informe al usuario final de las horas del centro de soporte y sobre opciones de soporte adicionales.

Nota: Para obtener más información acerca de la configuración de valores de Automatización de soporte, consulte la *Ayuda en línea*.

Servidores de enrutamiento de mensajes

Puede utilizar servidores de enrutamiento de mensajes (MRS) para gestionar varios servidores de control remoto, sobre la base de la ubicación geográfica del servidor local. El uso de las ayudas de MRS mejora el rendimiento durante las sesiones de asistencia. Cuando habilita MRS, la interfaz del analista de Automatización de soporte y el cliente de usuario final intentan conectarse al servidor (local) preferido de los analistas para uso compartido. Si la conexión falla, la sesión de uso compartido recae en el servidor predeterminado principal. El registro en vivo registra qué MRS se utiliza durante la sesión de asistencia.

Puede crear, actualizar, quitar, habilitar o deshabilitar un objeto del servidor de enrutamiento de mensajes.

Nota: Para obtener más información acerca de la configuración de servidores de enrutamiento de mensajes, consulte la *Ayuda en línea*.

Niveles de privacidad de Automatización de soporte

Los niveles de privacidad se utilizan para establecer las acciones que pueden realizar distintos usuarios finales para proteger la privacidad del usuario. Los niveles de privacidad están asociados con los roles de CA Service Desk Manager. Existen tres permisos predeterminados: Alto, Medio y Bajo, pero se pueden definir otros si es necesario. Puede agregar, actualizar y suprimir los niveles de privacidad que están disponibles para el usuario final.

Puede establecer el nombre del nivel de privacidad y su descripción. Puede definir las funciones habilitadas para las herramientas especificadas (explorador de archivos, registro remoto, ejecutar programa, etc.) en este nivel de privacidad.

Nota: Para obtener más información acerca de la configuración de niveles de privacidad de Automatización de soporte, consulte la *Ayuda en línea*.

Horas de Automatización de soporte

Puede establecer Automatización de soporte para que funcione en horas específicas o todo el tiempo. Puede gestionar estas horas de funcionamiento según las necesidades de los usuarios finales en el entorno de soporte. Los usuarios finales no pueden acceder a la funcionalidad de Automatización de soporte cuando ésta está cerrada. Puede realizar cambios rápidos para varios turnos en un solo paso.

Importante: puede asignar turnos tanto a las horas de Automatización de soporte como a colas individuales de asistencia en vivo. Los diferentes turnos que se asignan a colas individuales y horas de Automatización de soporte pueden causarles conflictos a analistas y usuarios finales en su entorno de soporte.

Nota: Para obtener más información acerca de la configuración de horas de Automatización de soporte, consulte la *Ayuda en línea*.

Cómo personalizar las herramientas de Automatización de soporte

Puede configurar las herramientas de Automatización de soporte para el entorno de soporte según las necesidades empresariales. La configuración le permite controlar la funcionalidad administrativa, como tareas automatizadas, conversaciones preestablecidas, credenciales predeterminadas y cláusulas de exención de responsabilidad.

- Personalizar la lista de tareas automatizadas y las clasificaciones que los analistas de Automatización de soporte utilizan para proporcionar soporte para los usuarios finales.
- Configurar las conversaciones preestablecidas para respuestas comunes para las preguntas y situaciones que se plantean con más frecuencia.
- Configurar las credenciales predeterminadas que permiten obtener acceso a un equipo del usuario final.
- Personalizar cláusulas de exención de responsabilidad que los usuarios finales visualizan antes de iniciar las tareas de autoservicio.

Nota: Para obtener más información acerca de la configuración de herramientas de Automatización de soporte, consulte la *Ayuda en línea*.

Tareas automatizadas

Una *tarea automatizada* es un conjunto de pasos que definen un proceso automatizado seguido por el analista o el usuario final. Los pasos de tareas automatizadas son rutinas escritas en VBScript o JavaScript que realizan acciones específicas en el equipo del analista o del usuario final. Con el editor de tareas automatizadas, se pueden crear nuevas tareas y pasos de tareas automatizadas. Las rutinas comunes incluyen recopilación de información de telemetría, diagnóstico de problemas e implementación de resoluciones.

El registro se actualiza durante la ejecución de una tarea automatizada. Este registro está vinculado con el registro de sesión de asistencia y tiene acceso desde éste. Las entradas en el registro de tareas automatizadas constan de un número de entradas de texto que incluyen marcas de tiempo. Estas entradas se crean mediante llamadas a Functions.LogMessage() o WScript.Echo().

Más información:

[Cómo implementar tareas automatizadas](#) (en la página 938)

Cómo configurar tareas automatizadas

El editor de tareas automatizadas se instala y configura para gestionar tareas automatizadas que los analistas de Automatización de soporte utilizan para proporcionar soporte para los usuarios finales. El usuario final puede iniciar una tarea automatizada en un documento de conocimiento y en la interfaz de autoservicio, o un analista ejecuta una tarea automatizada durante una sesión de asistencia. Las tareas automatizadas proporcionan a los analistas información detallada sobre el equipo de un usuario final. Puede crear tareas automatizadas de autoservicio que interactúan con el usuario final y procesan su entrada. Estas tareas pueden cambiar el sistema de archivos, el registro, descargar software de instalación, etc. Las tareas automatizadas se configuran de esta manera:

1. Instalar el editor de tareas automatizadas.

El instalador se ejecuta desde la siguiente ubicación en el medio de instalación:

casd.nt\SAScriptwriter

Nota: También puede copiar el instalador e implementarlo para los usuarios adecuados en el entorno de soporte.

Se instala el editor de tareas automatizadas.

2. Abrir el editor de tareas automatizadas.

La instalación del editor de tareas automatizadas crea un acceso directo en el escritorio.

3. Establecer los siguientes parámetros de conexión:

- a. Hacer clic en Herramientas, Servidor.

Aparecerá el cuadro de diálogo Configuración del servidor.

- b. Introducir el nombre de host y el puerto.

Puerto predeterminado: 8070

- c. Introduzca el nombre de usuario y la contraseña de un usuario con acceso de lectura/escritura al editor de tareas automatizadas, como por ejemplo un analista de Automatización de soporte.

- d. Haga clic en Probar.

- e. Haga clic en OK.

4. Crear las tareas automatizadas y cargarlas en el servidor.

Se pueden cargar tareas públicas o asignarlas a clientes y subclientes específicos.

Importante: sólo los roles del cliente proveedor de servicios que tienen el indicador Actualizar datos públicos habilitado puede cargar tareas y bibliotecas al servidor. Todo el contenido de la biblioteca de tareas y el contenido estático se almacena como datos públicos.

Cómo implementar tareas automatizadas

Puede utilizar las tareas automatizadas para ayudar a los usuarios finales en su entorno de soporte. Las tareas automatizadas completan acciones específicas en el equipo del usuario final, sin necesidad de que el analista o el usuario final realicen el proceso. Estos scripts le pueden ayudar a reunir información de telemetría, diagnosticar problemas del equipo e implementar resoluciones.

Para implementar tareas automatizadas, realice lo siguiente:

1. Identifique oportunidades para la automatización de soporte.

Se identifican los problemas comunes que los usuarios finales pueden encontrar, y se decide que se pueden automatizar algunas soluciones para reducir los costes de soporte.

2. Investigue la automatización de las soluciones posibles.

Se investigan las resoluciones para los problemas comunes y se reúnen datos sobre los procesos de diagnóstico que se planea utilizar.

3. Diseñe tareas para automatizar el soporte del usuario final.

Con el editor de tareas automatizadas, se diseña la experiencia de usuario final que se desea para cada tarea.

4. Implemente y pruebe las tareas automatizadas.

Las tareas automatizadas se prueban para comprobar que resuelven los problemas comunes encontrados en el entorno de soporte y que ayudan a reducir los costes de soporte.

5. Implemente y controle las tareas automatizadas.

Las tareas automatizadas se implementan para los usuarios finales del entorno permitiendo que los analistas las utilicen en las sesiones de soporte, o se pueden adjuntar scripts a los documentos de conocimiento.

Importante: Si está en un entorno multicliente y desea permitir a los analistas que carguen tareas y contenido de la biblioteca, el rol de éstos debe tener habilitada la opción *Actualizar datos públicos*.

Nota: CA puede brindar formación para la creación de tareas y componentes automatizados, como por ejemplo plantillas y bibliotecas de pasos de tareas automatizadas, que se puede utilizar en el entorno. Para obtener más información sobre el desarrollo de tareas automatizadas, póngase en contacto con *Servicios de CA*.

Administración de tareas automatizadas

Puede crear tareas automatizadas y asociarlas con el servidor. Necesita acceso de lectura/escritura a todas las tablas relacionadas con las tareas automatizadas para utilizar el editor de tareas automatizadas. Puede ejecutar funciones de gestión de usuarios con la aplicación, como asignar tareas automatizadas a roles y clientes.

Nota: Si es un analista proveedor de servicios que tiene acceso a clientes múltiples, puede seleccionar el contexto de cliente de cualquier operación de actualización de tareas con el servidor. También puede asignar una tarea automatizada como pública.

Implementación de tareas automatizadas

Después de crear y probar una tarea automatizada en el editor de tareas automatizadas, se la puede implementar para una clasificación en el servidor de CA Service Desk Manager para su uso en sesiones de asistencia o autoservicio. Algunas configuraciones que no forman parte de la definición de la tarea automatizada se establecen durante la implementación de la tarea.

Las tareas automatizadas se pueden cargar directamente al servidor o descargar de él, en el editor de tareas automatizadas. El cliente apropiado se selecciona al crear las clasificaciones de tareas automatizadas. Si carga scripts en el servidor, seleccione la clasificación o el cliente en los que tiene acceso, o establezca el script como público. También puede importar las tareas automatizadas a partir de archivos de XSDF y exportarlas a archivos de XSDF.

Importante: Si está en un entorno multicliente y desea permitir a los analistas que carguen tareas y contenido de la biblioteca, el rol de éstos debe tener habilitada la opción Actualizar datos públicos.

Carga de una tarea automatizada.

Se pueden cargar las tareas automatizadas creadas en la aplicación. Al seleccionar una tarea, se carga automáticamente todo el contenido dependiente, como por ejemplo las bibliotecas y el contenido estático.

Procedimiento para carga una tarea automatizada

1. Abra el editor de tareas automatizadas.

Aparece el editor de tareas de Automatización de soporte.

2. Seleccione la tarea automatizada que desea cargar.
3. Seleccione la clasificación en la que desea cargar la tarea.

Nota: Un usuario privilegiado en un entorno de multicliente puede seleccionar el cliente apropiado al cargar la tarea automatizada, o publicar la tarea.

4. En la barra de herramientas, seleccione el icono de carga de la tarea automatizada.

El editor de tareas de Automatización de soporte carga la tarea al servidor.

Edición de una tarea automatizada

Puede descargar tareas automatizadas del servidor y editarlas en el editor de tareas automatizadas. Cualquier contenido de la versión que sea más reciente que el que existe en el servidor se importa en la base de datos y se pone a disposición de los administradores de ese cliente.

Procedimiento para editar una tarea automatizada

1. Abra el editor de tareas automatizadas.
Aparece el editor de tareas de Automatización de soporte.
2. En la barra de herramientas, seleccione el icono de carga de la tarea automatizada.
Aparece el panel Abrir tarea automatizada desde el servidor.
3. Seleccione la tarea automatizada que desea descargar.
Nota: Un usuario privilegiado en un entorno de multicliente puede editar tareas automatizadas públicas o específicas de cliente.
4. Haga clic en Abrir tarea.
El editor de tareas de Automatización de soporte descarga la tarea al cliente y la abre en la aplicación.
La descarga crea un archivo de texto en el equipo del autor de la tarea que contiene el contenido dependiente.

Credenciales de tareas automatizadas

Se puede ejecutar una tarea automatizada para la que se necesitan privilegios administrativos para la ejecución, por ejemplo al realizar una instalación de software, realizando estas acciones:

- Definir credenciales predeterminadas para el cliente y configurar la tarea automatizada para que utilice los credenciales predeterminadas en la administración de la tarea automatizada.
- Definir credenciales predeterminadas para el cliente y seleccionar que se utilizará el cuadro de diálogo Ejecutar como en la ventana Sesión de asistencia.
- Definir credenciales de tareas automatizadas para la tarea y especificar que se utilizará el cuadro de diálogo Ejecutar como en la ventana Sesión de asistencia.
- Especificar las credenciales en el cuadro de diálogo Ejecutar como en la ventana Sesión de asistencia.

Asignaciones de roles

Los roles apropiados (por ejemplo, analista, administrador) se asignan para utilizar la tarea automatizada. Las tareas automatizadas individuales se asignan a los roles seleccionados para limitar las tareas automatizadas exclusivamente a los analistas del rol asignado. Se pueden gestionar diferentes conjuntos de habilidades o niveles de experiencia dentro de la organización de soporte.

Los roles se pueden gestionar a nivel de tarea, seleccionando tareas que se ejecutan con frecuencia, como por ejemplo los diagnósticos, para que se ejecuten automáticamente cuando el usuario final ingresa a una sesión.

Asignar un nivel de acceso a un rol

Los niveles de acceso de Automatización de soporte se pueden asignar a los roles existentes de CA Service Desk Manager en el entorno.

Procedimiento para asignar un nivel de acceso a un rol

1. Seleccione Gestión de roles y seguridad, Gestión de roles, Lista de roles en la ficha Administración.
Aparecerá la página Lista de roles.
2. Haga clic en el rol al que desea asignar el nivel de acceso, por ejemplo Administrador.
Aparecerá la página Detalles del rol.
3. Haga clic en Editar.
Aparecerá la página Actualizar rol.
4. En la ficha Autorización, seleccione el nivel de acceso que ha creado en la lista desplegable del Acceso al servicio de automatización de soporte.
Aparecerá la página Detalles del rol. Verifique que el acceso de Automatización de soporte se asigna al rol.

Administración de conversación preestablecida

Puede crear respuestas comunes a las preguntas y situaciones más frecuentes. En lugar de escribir repetidamente la misma información, puede guardar una respuesta y utilizarla en otras sesiones de conversación.

Puede enviar valores preestablecidos a los usuarios finales en forma automática durante el inicio de cada sesión, por ejemplo un saludo. También puede completar en forma automática los valores preestablecidos con información específica de la sesión actual, por ejemplo el nombre del analista.

En una sesión de asistencia se pueden utilizar los siguientes tipos de valores preestablecidos:

Conversación preestablecida

Identifica una respuesta de texto utilizada frecuentemente para una pregunta del usuario final.

URL preestablecida

Identifica una URL utilizada frecuentemente a la que el usuario final puede acceder.

Puede encontrar cada conversación preestablecida. La conversación preestablecida se sincroniza con la ubicación del usuario final para que éste reciba los valores preestablecidos localizados correctos.

Cómo gestionar conversaciones preestablecidas

Puede utilizar respuestas predefinidas para las preguntas y situaciones más frecuentes.

1. Entender las sesiones de asistencia típicas en la organización.
2. Crear conversaciones y URL preestablecidas basadas en las necesidades de la organización
3. Especificar si las conversaciones y URL preestablecidas se deben poner a disposición como específicas de los clientes o públicas.
4. (Opcional) Duplicar la estructura de árbol preestablecida para gestionar entornos localizados.
5. Enviar las conversaciones y URL preestablecidas durante una sesión de asistencia.

Nota: Para obtener más información acerca de la configuración de conversaciones preestablecidas, consulte la *Ayuda en línea*.

Credenciales predeterminadas

Puede ejecutar tareas automatizadas en el equipo del usuario final incluso si éste normalmente no tiene derechos de acceso al sistema para realizar estas actividades. Si el usuario final actual no tiene derechos administrativos para ver información del sistema sobre su equipo, puede ejecutar una tarea automatizada restringida utilizando credenciales predeterminadas para obtener acceso.

Nota: Para obtener más información acerca de la configuración de credenciales predeterminadas, consulte la *Ayuda en línea*.

Cláusulas de exención de responsabilidad

Cuando los usuarios finales inician tareas de autoservicio, se les presenta el texto de cláusula de exención de responsabilidad que deben aceptar antes de poder continuar.

Puede crear, actualizar y suprimir los objetos de negocio de la cláusula de exención de responsabilidad.

Nota: Para obtener más información acerca de la configuración de cláusulas de exención de responsabilidad de Automatización de soporte, consulte la *Ayuda en línea*.

Administración del registro de sesión

El registro de sesión le permite ver todas las acciones que realiza el analista durante una sesión de asistencia, como por ejemplo las herramientas utilizadas y los detalles de la conversación (con excepción de los susurros). Puede imprimir o enviar por correo electrónico al usuario final el registro de sesión. Los usuarios finales también pueden ver y guardar el registro, pero no pueden modificarlo.

Visualizar el registro de sesión

Todas las acciones que se ejecutan durante la sesión de asistencia, como por ejemplo el diálogo de conversación (con excepción de las conversaciones de susurros), los resultados de las tareas automatizadas y la utilización de herramientas específicas de la interfaz de analista de Automatización de soporte, actualizan el registro de sesión.

Procedimiento para ver el registro de sesión

1. Abra la vista de sesión activa.
Aparece la página Sesión activa.
2. Seleccione Registro de sesión en la barra de herramientas o en el menú Sesiones.
Aparece la página Registro de sesión.
3. Haga clic en Actualizar ahora.
Se actualiza la página.
4. (Opcional) Seleccione la casilla de verificación Actualización automática.
5. (Opcional) Haga clic en Guardar registro en disco.
Aparece el cuadro de diálogo Guardar. Puede guardar localmente el registro de sesión como un archivo HTML.

Informes de Automatización de soporte

CA Business Intelligence instala un conjunto de informes de Automatización de soporte predefinidos. Durante la instalación, CA Service Desk Manager implementa automáticamente estos informes en el servidor de BusinessObjects.

Los roles de administrador de Automatización de soporte y analista de Automatización de soporte pueden utilizar BusinessObjects InfoView para ver información detallada y de resumen de:

- Métricas de inicio de sesión de analista
- Métricas de sesiones de asistencia
- Métricas de entradas de colas
- Métricas de ejecución de tareas automatizadas
- Uso de herramientas por categoría de ticket
- Datos en tiempo real sobre usuarios finales puestos en colas de soporte, sesiones de asistencia activas, y analistas activos (conectados).

Nota: Para obtener más información acerca del uso de BusinessObjects InfoView, consulte la información de CA Business Intelligence en la *Ayuda en línea*.

Apéndice A: Descripciones de los campos de vista

Esta sección contiene los siguientes temas:

[Descripciones de los campos de vista](#) (en la página 948)

[View Act Log](#) (en la página 948)

[View Audit Assignee](#) (en la página 950)

[View Audit Group](#) (en la página 950)

[View Audit Priority](#) (en la página 951)

[View Audit Status](#) (en la página 952)

[View Change Act Log](#) (en la página 952)

[View Change](#) (en la página 954)

[View Change to Assets](#) (en la página 959)

[View Change to Change Act Log](#) (en la página 959)

[View Change to Change WF](#) (en la página 961)

[View Change to Properties](#) (en la página 963)

[View Contact Full](#) (en la página 964)

[View Contact to Environment](#) (en la página 967)

[View Group](#) (en la página 968)

[View Group To Contact](#) (en la página 969)

[View Issue](#) (en la página 969)

[View Issue Act Log](#) (en la página 974)

[View Issue to Assets](#) (en la página 975)

[View Issue to Issue Act Log](#) (en la página 976)

[View Change to Requests](#) (en la página 977)

[View Issue to Issue WF](#) (en la página 981)

[View Issue to Properties](#) (en la página 983)

[View Request](#) (en la página 984)

[View Request to Act Log](#) (en la página 989)

[View Request to Properties](#) (en la página 990)

Descripciones de los campos de vista

Puede utilizar la información de descripción de campo en las vistas básica y avanzada que se suministran con CA Service Desk Manager.

Los puntos siguientes se aplican a muchas de las tablas:

- Debe activar la función de registro de auditoría, que se encuentra en Administración (de Service Desk) > Gestor de opciones > Registro de auditoría, para poder ver los datos en las vistas avanzadas.
- Nota:** Para obtener más información sobre el registro de auditoría, consulte la *Ayuda en línea*.
- pdmtime hace referencia a los campos de fecha y hora que encuentran en formato GMT (número de segundos transcurridos desde 1/1/1970).
 - Los términos "solicitud de cambios" y "orden de cambio" son intercambiables.

Más información:

[Generación de informes en CA Service Desk Manager](#) (en la página 767)

View_Act_Log

Se trata de una vista básica de la tabla del registro de actividades de las solicitudes. En ella también figuran el tipo de actividad así como el nombre completo de los analistas. Se ha unido la tabla del registro de actividades (act_log) con la tabla del tipo de actividad (act_type) y la tabla de contactos (ca_contact) para obtener el tipo de actividad real de cada entrada del registro de actividades y el analista que ha llevado a cabo la actividad. Al final de esta lista aparecen los campos extraídos de las uniones, lo que puede resultar de utilidad.

Campo	Observaciones
ID	act_log.id: identificador exclusivo para el registro en la tabla act_log.
persid	act_log.persid: identificador exclusivo para el registro en la tabla act_log, precedido por el identificador de objeto (alg para la tabla act_log) y dos puntos.
call_req_id	act_log.call_req_id: puntero al persid de solicitud de llamada a la que pertenece la actividad. act_log.call_req_id = call_req.persid.
last_mod_dt	act_log.last_mod_dt: fecha y hora de la última modificación (pdmtime).
time_spent	act_log.time_spent: tiempo empleado en la actividad, almacenado

Campo	Observaciones
	como el número total de segundos. por ejemplo, 80 = 1 minuto y 20 segundos.
time_stamp	act_log.time_stamp: fecha y hora de la actividad susceptible de modificación por el usuario (pdmtime).
system_time	act_log.system_time: fecha y hora de creación del registro (pdmtime).
analista	act_log.analyst: puntero UUID al UUID del contacto para obtener el analista que realizó la actividad. act_log.analyst = ca_contact.contact_uuid.
descripción	act_log.description: texto descriptivo de la actividad susceptible de modificación por parte del usuario.
action_desc	act_log.action_desc: texto descriptivo de la acción automatizada que no es susceptible de modificación por parte del usuario.
tipo	act_log.type: puntero de texto a un registro de la tabla de tipos de actividades. Por ejemplo, act_log.type = act_type.code.
knowledge_session	act_log.knowledge_session: identificador de una sesión en particular de un usuario concreto.
knowledge_tool	act_log.knowledge_tool: indicador de la herramienta de conocimiento empleada para la búsqueda como, por ejemplo, NLS_FAQ, EXPERT, etc.
interno	act_log.internal: indicador en forma de entero (1 o 0) que señala si la entrada del registro pueden consultarla todos los usuarios o sólo es para uso interno.
activity_type	act_type.sym: tipo de actividad derivado de act_log.type = act_type.code.
analyst_lastname	View_Contact_Full.last_name: apellidos del analista derivados de act_log.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: nombre del analista.
analyst_middlename	View_Contact_Full.middle_name: segundo nombre del analista.

View_Audit_Assignee

Se trata de una vista avanzada del registro de auditoría donde se realiza el seguimiento de los asignatarios. Esta vista refleja el tiempo que transcurre entre los cambios del asignatario para las solicitudes y las órdenes de cambios. Si, en las solicitudes o en las órdenes de cambios, se cambia de un asignatario concreto a uno nulo y, después, del nulo a otro asignatario en particular, la duración del asignatario nulo no se refleja en la vista. La vista muestra los campos siguientes tanto para las solicitudes como para las órdenes de cambios. Puede haber más de una entrada por cada audobj_uniqueid (solicitud u orden de cambios).

Campo	Observaciones
audobj_uniqueid	audit_log.audobj_uniqueid: ID exclusivo de objeto del registro de auditoría que representa el valor de chg.id o de call_req.id.
from_val	audit_log.attr_after_val: valor de asignatario 'cambiado de'.
to_val	audit_log.attr_after_val: valor de asignatario 'cambiado a'.
from_time	audit_log.attr_from_time: hora de inicio en que se asignó el asignatario (pdmtime).
to_time	audit_log.attr_from_time: hora final en que se asignó el mismo asignatario (pdmtime).

View_Audit_Group

Se trata de una vista avanzada del registro de auditoría donde se realiza el seguimiento de los grupos. Esta vista refleja el tiempo que transcurre entre los cambios del grupo para las solicitudes y las órdenes de cambios. Si, en las solicitudes o en las órdenes de cambios, se cambia de un grupo concreto a uno nulo y, después, del nulo a otro grupo en particular, la duración del grupo nulo no se refleja en la vista. La vista muestra los campos siguientes tanto para las solicitudes como para las órdenes de cambios. Puede haber más de una entrada por cada audobj_uniqueid (solicitud u orden de cambios).

Campo	Observaciones
audobj_uniqueid	audit_log.audobj_uniqueid: ID exclusivo de objeto del registro de auditoría que representa el valor de chg.id o de call_req.id.
from_val	audit_log.attr_after_val: valor de grupo 'cambiado de'.

Campo	Observaciones
to_val	audit_log.attr_after_val: valor de grupo 'cambiado a'.
from_time	audit_log.attr_from_time: hora de inicio en que se asignó el grupo (pdmtime).
to_time	audit_log.attr_from_time: hora final en que se asignó el mismo grupo (pdmtime).

View_Audit_Priority

Se trata de una vista avanzada del registro de auditoría donde se realiza el seguimiento de la prioridad. Esta vista refleja el tiempo que transcurre entre los cambios de la prioridad para las solicitudes y las órdenes de cambios. La vista muestra los campos siguientes tanto para las solicitudes como para las órdenes de cambios. Puede haber más de una entrada por cada audobj_uniqueid (solicitud u orden de cambios).

Campo	Observaciones
audobj_uniqueid	audit_log.audobj_uniqueid: ID exclusivo de objeto de auditoría que representa el valor de chg.id de una orden de cambio o de call_req.id de una solicitud.
from_val	audit_log.attr_after_val: valor de prioridad 'cambiado de'.
to_val	audit_log.attr_after_val: valor de prioridad 'cambiado a'.
from_time	audit_log.attr_from_time: hora de inicio en que la prioridad se encontraba en un estado determinado (pdmtime).
to_time	audit_log.attr_from_time: hora final en que la prioridad se encontraba en el mismo estado (pdmtime).

View_Audit_Status

Se trata de una vista avanzada del registro de auditoría donde se realiza el seguimiento del estado. Esta vista refleja el tiempo que transcurre entre los cambios del estado para las solicitudes y las órdenes de cambios. La vista muestra los campos siguientes tanto para las solicitudes como para las órdenes de cambios. Puede haber más de una entrada por cada audobj_uniqueid (solicitud u orden de cambios).

Campo	Observaciones
audobj_uniqueid	audit_log.audobj_uniqueid: ID exclusivo de objeto de auditoría que representa el valor de chg.id de una orden de cambio o de call_req.id de una solicitud.
from_val	audit_log.attr_after_val: valor de prioridad 'cambiado de'.
to_val	audit_log.attr_after_val: valor de prioridad 'cambiado a'.
from_time	audit_log.attr_after_time: hora de inicio en que el estado se encontraba en un estado determinado (pdmtime).
to_time	audit_log.attr_after_time: hora final en que el estado se encontraba en el mismo estado (pdmtime).

View_Change_Act_Log

Se trata de una vista básica de todos los registros de actividades de las órdenes de cambios. Esta vista aúna la tabla del registro de actividades de solicitudes de cambios (chgalg) y las tablas del tipo de actividad (act_type) y de contactos (ca_contact) para obtener datos más significativos como, por ejemplo, la descripción del tipo de actividad real y el nombre completo del analista que ha llevado a cabo la actividad.

Campo	Observaciones
ID	chgalg.id: identificador exclusivo para el registro en la tabla chgalg.
persid	chgalg.persid: identificador exclusivo para el registro en la tabla chgalg precedido por el identificador de objeto (chgalg para la tabla chgalg) y dos puntos.
change_id	chgalg.change_id: puntero al ID de la orden de cambio a la que pertenece la actividad.

Campo	Observaciones
	chgalg.change_id = chgalg.id
last_mod_dt	chgalg.last_mod_dt: fecha y hora de la última modificación (pdmtime).
time_spent	chgalg.time_spent: tiempo empleado en la actividad, almacenado como el número total de segundos. por ejemplo, 80 = 1 minuto y 20 segundos.
time_stamp	chgalg.time_stamp: fecha y hora de la actividad susceptible de modificación por el usuario (pdmtime).
system_time	chgalg.system_time: fecha y hora de creación del registro (pdmtime).
analista	chgalg.analyst: puntero UUID al UUID del contacto para obtener el analista que realizó la actividad. chgalg.analyst = ca_contact.contact_uuid
descripción	chgalg.description: texto descriptivo de la actividad susceptible de modificación por parte del usuario.
action_desc	chgalg.action_desc: texto descriptivo de la acción automatizada que no es susceptible de modificación por parte del usuario.
tipo	chgalg.type: puntero de texto a un registro de la tabla de tipos de actividades. chgalg.type = act_type.code
interno	chgalg.internal: indicador en forma de entero (1 ó 0), que señala si la entrada del registro pueden consultarla todos los usuarios o sólo es para uso interno.
knowledge_session	chgalg.knowledge_session: identificador de una sesión en particular de un usuario concreto.
knowledge_tool	chgalg.knowledge_tool: indicador de la herramienta de conocimiento empleada para la búsqueda como, por ejemplo, NLS_FAQ, EXPERT, etc.
analyst_lastname	View_Contact_Full.last_name: apellidos del analista derivados de chgalg.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: nombre del analista.
analyst_middlename	View_Contact_Full.middle_name: segundo nombre del analista.
activity_type	act_type.sym: tipo de actividad al que hace referencia chgalg.type = act_type.code.

View_Change

Se trata de una vista básica de todas las órdenes de cambios donde figuran datos como el estado, la prioridad, la categoría, las organizaciones, el nombre completo del usuario final afectado, el nombre completo del solicitante, el nombre completo del asignatario, el nombre del grupo, el ID del grupo, etc. En ella se ha unido la tabla de solicitudes de cambio (chg) con muchas otras tablas a fin de obtener datos más significativos sobre las órdenes de cambios.

Campo	Observaciones
ID	chg.id: identificador exclusivo para el registro en la tabla chg.
persid	chg.persid: identificador exclusivo para el registro en la tabla chg, precedido por el identificador de objeto (chg para la tabla chg) y dos puntos.
chg_ref_num	chg.chg_ref_num: número de referencia de la orden de cambio que emplean los analistas y los clientes para hacer referencia a una orden de cambio en particular.
descripción	chg.description: descripción completa de la orden de cambio redactada por un analista o un cliente.
estado	chg.status: identificador exclusivo del estado de la orden de cambio, que es un puntero a la tabla chgstat: chg.status = chgstat.code.
active_flag	chg.active_flag: indicador en forma de entero que determina si el registro del cambio está activo o no (1 o 0).
start_date	chg.start_date: fecha en la que la tarea pasa por primera vez al estado pendiente (pdmtime).
open_date	chg.open_date: fecha de creación de la orden de cambio (pdmtime).
last_mod_dt	chg.last_mod_dt: fecha de la última modificación (pdmtime).
last_mod_by	chg.last_mod_by: puntero al UUID del contacto que modificó por última vez la orden de cambio. chg.last_mod_by = ca_contact.contact_uuid.
close_date	chg.close_date: fecha en la que se estableció la orden de cambio como inactiva (pdmtime).
resolve_date	chg.resolve_date: fecha en la que se estableció la orden de cambio en un estado configurado para indicar que el cambio se ha resuelto (pdmtime).
rootcause	chg.rootcause: puntero al registro de la tabla rootcause que representa la situación original que exigía la ejecución de esta orden de cambio.

Campo	Observaciones
	chg.rootcause = rootcause.id.
est_total_time	chg.est_total_time: tiempo total estimado (pdmtime) para finalizar el cambio.
actual_total_time	chg.actual_total_time: tiempo total real (pdmtime) que se tardó en finalizar el cambio.
log_agent	chg.log_agent: identificador exclusivo binario que hace referencia a la persona de la tabla ca_contact que es el creador original del cambio. chg.log_agent = ca_contact.contact_uuid.
asignado	chg.assignee: puntero al UUID del contacto que está asignado actualmente a la orden de cambio. chg.assignee = ca_contact.contact_uuid.
organización	chg.organization: puntero al UUID de la organización interna que representa la organización a la que pertenece esta orden de cambio. chg.organization = ca_organization.organization_uuid.
group_id	chg.group_id: puntero al UUID del contacto que representa el grupo que está asignado actualmente a la orden de cambio. chg.group_id = ca_contact.contact_uuid.
affected_contact	chg.affected_contact: puntero al UUID del contacto que representa el contacto afectado por la orden de cambio. chg.affected_contact = ca_contact.contact_uuid.
solicitante	chg.requestor: puntero al UUID del contacto que representa la persona que solicitó el cambio. chg.requestor = ca_contact.contact_uuid.
categoría	chg.category: puntero al código de la categoría de cambio para obtener la categoría en la que entra este cambio. chg.category = chgcat.code.
prioridad	chg.priority: puntero al valor de prioridad que representa la prioridad en la que entra este cambio. chg.priority = pri.enum.
need_by	chg.need_by: fecha que indica para cuándo necesita el usuario affected_end_user tener finalizado el cambio (pdmtime).
est_comp_date	chg.est_comp_date: fecha de finalización estimada (pdmtime) de la orden de cambio.
actual_comp_date	fecha de finalización real (pdmtime) de la orden de cambios.
est_cost	chg.est_cost: coste estimado de la orden de cambio.
actual_cost	chg.actual_cost: coste real de la implementación de esta orden de cambio.

Campo	Observaciones
justificación	chg.justification: campo de texto para que el solicitante documente los motivos por los que es preciso el cambio.
backout_plan	chg.backout_plan: campo de texto para que el analista documente el plan de retroceso del cambio.
impact	chg.impact: puntero al registro de una tabla impact que indica el ámbito de los recursos a los que afecta este cambio. chg.impact = impact.enum.
principal	chg.impact: puntero al ID de otra solicitud de cambio que permite la creación de una jerarquía de órdenes de cambio. chg.parent = chg.id.
dificultad	chg.effort: campo de texto que explica el plan para implementar esta orden de cambio.
support_lev	chg.support_lev: puntero al registro de descripción del servicio que automatiza algunas de las restricciones para las que se debe finalizar el cambio. chg.support_lev = srv_desc.code.
template_name	chg.template_name: nombre de la plantilla de la orden de cambio y puntero a la misma. chg.template_name = chg_template.template_name.
sla_violation	chg.sla_violation: entero que representa el recuento de veces en que se ha infringido el acuerdo de nivel de servicio adjunto al cambio.
predicted_sla_viol	chg.predicted_sla_viol (r5.5): campo destinado a la tecnología relacionada con Neugent.
macro_predict_viol	chg.macro_predict_viol (r5.5): campo destinado a la tecnología relacionada con Neugent.
created_via	chg.created_via: puntero al registro de la tabla interface que indica en qué interfaz se ha originado la orden de cambio. chg.created_via = interface.id
call_back_date	campo de fecha y hora (pdmtime) que indica la fecha y la hora futuras cuando hay que ponerse en contacto con el solicitante.
call_back_flag	chg.call_back_flag: indicador booleano que se presenta al usuario como casilla de verificación y que indica si hay que enviar una notificación al analista en la fecha de chg.call_back_date.
string1	Campo de texto susceptible de definición por parte del usuario.
string2	Campo de texto susceptible de definición por parte del usuario.
string3	Campo de texto susceptible de definición por parte del usuario.
string4	Campo de texto susceptible de definición por parte del usuario.

Campo	Observaciones
string5	Campo de texto susceptible de definición por parte del usuario.
string6	Campo de texto susceptible de definición por parte del usuario.
service_date	chg.service_date: fecha y hora (pdmtime) cuando se prevé que el distribuidor externo atienda esta orden de cambio.
service_num	chg.service_num: campo de texto para documentar el número de orden de compra o la orden de servicio del distribuidor externo.
producto	chg.product: puntero al registro de la tabla product que indica el producto al que afecta el cambio. chg.product = product.id.
acciones	chg.actions: campo de texto de gran tamaño para documentar las acciones.
type_of_contact	chg.type_of_contact: puntero al registro de la tabla toc que indica la categorización general de la perspectiva del usuario affected_end_user de la orden de cambio. chg.type_of_contact = toc.id.
reporting_method	chg.reporting_method: puntero al registro de la tabla repmeth que clasifica el origen de la orden de cambio y que selecciona la persona que la crea. chg.reporting_method = repmeth.id.
person_contacting	chg.person_contacting: puntero al registro de la tabla perscon que indica el rol del solicitante o el usuario affected_end_user. chg.person_contacting = perscon.id
status_name	chgstat.sym: descripción del estado como lo ve el usuario. chg.status = chgstat.code.
priority_num	pri.sym: descripción de la prioridad como la ve el usuario. chg.priority = pri.enum.
category_name	chgcat.sym: nombre de la categoría de cambio como lo ve el usuario. chg.category = chgcat.code.
organization_name	ca_organization.org_name: nombre de la organización como lo ve el usuario. chg.organization = ca_organization.organization_uuid.
affected_end_user_lastname	ca_contact.last_name: apellidos del usuario final afectado. chg.affected_end_user = ca_contact.contact_uuid.
affected_end_user_firstname	ca_contact.first_name: nombre del usuario final afectado. chg.affected_end_user = ca_contact.contact_uuid.
affected_end_user_middlename	ca_contact.middle_name: segundo nombre del usuario final afectado. chg.affected_end_user = ca_contact.contact_uuid.

Campo	Observaciones
requester_lastname	ca_contact.last_name: apellidos del solicitante. chg.requestor = ca_contact.contact_uuid.
requester_firstname	ca_contact.first_name: nombre del solicitante. chg.requestor = ca_contact.contact_uuid.
requester_middlename	ca_contact.middle_name: segundo nombre del solicitante. chg.requestor = ca_contact.contact_uuid.
negocio	ca_organization.org_name: nombre de la organización del solicitante como lo ven los usuarios. chg.requestor = ca_organization.organization_uuid.
assignee_lastname	ca_contact.last_name: apellidos del asignatario. chg.assignee = ca_contact.contact_uuid.
assignee_firstname	ca_contact.first_name: nombre del asignatario. chg.assignee = ca_contact.contact_uuid.
assignee_middlename	ca_contact.middle_name: segundo nombre del asignatario. chg.assignee = ca_contact.contact_uuid.
groupID	ca_contact.contact_uuid: representación binaria del ID interno empleado para el grupo asignado a esta orden de cambio. chg.group_id = ca_contact.contact_uuid.
group_name	ca_contact.last_name: nombre del grupo asignado a esta orden de cambio. chg.group = ca_contact.contact_uuid.
service_type	srv_desc.sym: nombre del tipo de servicio aplicado a esta orden de cambio. chg.support_lev = srv_desc.code.
impact_num	impact.sym: descripción del impacto como lo ve el usuario. chg.impact = impact.enum.
product_sym	product.sym: descripción del producto como lo ve el usuario. chg.product = product.id.
type_of_contact_sym	toc.sym: descripción del tipo de contacto como lo ve el usuario. chg.type_of_contact = toc.id.
rpting_method_sym	repmeth.sym: descripción del método de presentación de informes como lo ve el usuario. chg.reporting_method = repmeth.id.
person_contacting_sym	perscon.sym: descripción de la persona de contacto como la ve el usuario. chg.person_contacting = perscon.id

View_Change_to_Assets

La siguiente lista de campos es una vista básica de las órdenes de cambio y sus activos. La tabla de solicitudes de cambios (chg) se une de forma indirecta con la tabla de recursos de red (ca_owned_resource) para obtener una lista de los activos de las órdenes de cambios. Es posible que en esta vista no figuren todas las órdenes de cambio, en particular si no disponen de activos.

Campo	Observaciones
View_Change.*	Todos los campos antes enumerados para la vista View_Change.
assetID	ca_owned_resource.own_resource_uuid: campo binario que actúa como identificador exclusivo interno que no cambia para el registro del activo.
asset_serial_num	ca_owned_resource.serial_number: número de serie del registro del activo.
asset_class	ca_resource_class.name: descripción breve de la clase a la que pertenece el activo. ca_owned_resource.resource_class = ca_resource_class.id.
asset_family	ca_resource_family.name: familia de activos a la que pertenece el activo. ca_owned_resource.resource_class = ca_resource_class.id Y ca_resource_class.family_id = ca_resource_family.id.
asset_name	ca_owned_resource.resource_name: nombre de red por el que se conoce el activo.

View_Change_to_Change_Act_Log

Se trata de una vista básica de todas las órdenes de cambios y de los registros de actividades que las acompañan. Esta vista aúna la vista View_Change y el registro de actividades de las órdenes de cambios (chgalg) para ofrecer información detallada sobre las órdenes de cambios y sus registros de actividades.

Campo	Observaciones
View_Change.*	Muestra todos los campos antes enumerados para la vista View_Change.
chgalg_id	chgalg.id: identificador exclusivo para el registro en la tabla chgalg.
chgalg_persid	chgalg.persid: identificador exclusivo para el registro en la tabla chgalg precedido por el identificador de objeto (chgalg para la

Campo	Observaciones
	tabla chgalg) y dos puntos.
change_id	chgalg.change_id: puntero para cambiar el ID de la orden a la que pertenece esta actividad. chgalg.change_id = chgalg.id
chgalg_last_mod_dt	chgalg.last_mod_dt: fecha y hora de la última modificación (pdmtime).
time_spent	chgalg.time_spent: tiempo empleado en la actividad, almacenado como el número total de segundos. por ejemplo, 80 = 1 minuto y 20 segundos.
time_stamp	chgalg.time_stamp: fecha y hora de la actividad susceptible de modificación por el usuario (pdmtime).
system_time	chgalg.system_time: fecha y hora de creación del registro (pdmtime).
analista	chgalg.analyst: puntero UUID al UUID del contacto para obtener el analista que realizó la actividad. chgalg.analyst = ca_contact.contact_uuid
chgalg_description	chgalg.description: texto descriptivo de la actividad susceptible de modificación por parte del usuario.
action_desc	chgalg.action_desc: texto descriptivo de la acción automatizada que no es susceptible de modificación por parte del usuario.
tipo	chgalg.type: puntero de texto a un registro de la tabla de tipos de actividades. chgalg.type = act_type.code
interno	chgalg.internal: indicador en forma de entero (1 ó 0), que señala si la entrada del registro pueden consultarla todos los usuarios o sólo es para uso interno.
knowledge_session	chgalg.knowledge_session: identificador de una sesión en particular de un usuario concreto.
knowledge_tool	chgalg.knowledge_tool: indicador de la herramienta de conocimiento empleada para la búsqueda como, por ejemplo, NLS_FAQ, EXPERT, etc.
chgalg_analyst_id	chgalg.analyst: puntero UUID al UUID del contacto para obtener el analista que realizó la actividad. chgalg.analyst = ca_contact.contact_uuid

View_Change_to_Change_WF

Esta vista es el resultado de aunar la vista View_Change y la tabla de tareas de workflow (wf) para ofrecer una vista básica de las órdenes de cambios y sus tareas de workflow. Es posible que no figuren todas las órdenes de cambios, en particular si no se les ha asignado ninguna tarea de workflow.

Campo	Observaciones
View_Change.*	Muestra todos los campos antes enumerados para la vista View_Change.
wf_id	wf.id: identificador exclusivo para el registro en la tabla wf.
wf_persid	wf.persid: identificador exclusivo para el registro en la tabla wf precedido por el identificador de objeto (wf para la tabla wf) y dos puntos.
del	wf.del: indicador booleano. Indica si el registro se debe mostrar al usuario.
object_type	wf.object_type: nombre de fábrica empleado para identificar el tipo de registro (por ejemplo, chg) al que se adjunta esta tarea de workflow.
object_id	wf.object_id: identificador exclusivo empleado para identificar el registro específico al que se adjunta esta tarea de workflow. wf.object_id = chg.id.
tarea	wf.task: identificador que hace referencia al tipo de tarea que representa el registro. wf.task = tskty.code.
wf_template	wf.wf_template: identificador que hace referencia a la plantilla a partir de la que se creó el registro de la tarea de workflow. wf.wf_template = wftpl.id.
secuencia	wf.sequence: entero que indica el orden en el que CA Service Desk Manager debe mostrar y ejecutar el registro de esta tarea de workflow en particular (por, ejemplo, ascendente).
wf_status	wf.status: identificador que hace referencia al registro tskstat que indica el estado actual de esta tarea de workflow. wf.status = tskstat.code
group_task	wf.group_task: valor booleano que indica si la tarea pertenece a algún grupo.
activo	wf.asset: identificador UUID (binario) que hace referencia a un registro de la tabla ca_owned_resource. wf.asset = ca_owned_resource.own_resource_uuid.
creador	wf.creator: identificador UUID (binario) que hace referencia a un registro de la tabla ca_contact. Indica la persona que ha creado la

Campo	Observaciones
	tarea de workflow. wf.creator = ca_contact.contact_uuid.
date_created	wf.date_created: fecha o indicación de tiempo que señala cuándo se creó esta tarea de workflow (pdmtime).
wf_assignee	wf.assignee: identificador UUID (binario) que hace referencia a un registro de la tabla ca_contact. Indica la persona que está asignada actualmente a la tarea de workflow. wf.assignee = ca_contact.contact_uuid.
done_by	wf.done_by: identificador UUID (binario) que hace referencia a un registro de la tabla ca_contact. Indica la persona que ha finalizado o aprobado la tarea de workflow. wf.done_by = ca_contact.contact_uuid.
wf_start_date	wf_start_date: sello de hora que indica cuándo se ha movido la tarea de workflow a un estado activo (pdmtime).
wf_est_comp_date	wf.est_comp_date: indicación de tiempo (pdmtime) que señala cuándo cree el usuario que estará finalizada la tarea.
est_duration	wf.est_duration: duración estimada de la tarea de workflow.
completion_date	wf.completion_dat: indicación de tiempo (pdmtime) que señala cuándo se finalizó la tarea de workflow.
actual_duration	wf.actual_duration: tiempo real que se tardó en finalizar la tarea de workflow.
wf_est_cost	wf.est_cost: coste estimado de la tarea de workflow.
coste	wf.cost: coste real necesario para finalizar la tarea de workflow.
wf_description	wf.description: descripción de la tarea de workflow.
wf_last_mod_dt	wf.last_mod_dt: indicación de tiempo (pdmtime) que señala cuándo se modificó por última vez la tarea de workflow.
wf_last_mod_by	wf.last_mod_by: identificador exclusivo UUID (binario) que hace referencia al registro de la tabla de contactos, que indica la última persona que realizó algún cambio en la tarea de workflow. wf.last_mod_by = ca_contact.contact_uuid.

View_Change_to_Properties

Esta vista es el resultado de aunar la vista View_Change y la tabla de propiedades (prp) para ofrecer una vista básica de las órdenes de cambios y sus propiedades asignadas. Es posible que no figuren todas las órdenes de cambios, en particular si no se les ha asignado ninguna propiedad.

Campo	Observaciones
View_Change.*	Muestra todos los campos antes enumerados para la vista View_Change.
prp_id	prp.id: entero que es el identificador exclusivo para el registro de la propiedad.
prp_persid	prp.persid: identificador exclusivo para el registro en la tabla wf, precedido por el identificador de objeto (prp para prp) y dos puntos.
object_type	prp.object_type: nombre de fábrica empleado para identificar el tipo de registro (por ejemplo, chg) al que se adjunta el registro de la propiedad.
object_id	prp.object_id: identificador exclusivo empleado para identificar el registro específico al que se adjunta esta propiedad. prp.object_id = chg.id
secuencia	prp.sequence: entero que indica el orden en el que CA Service Desk Manager debe mostrar el registro de esta propiedad en particular (por, ejemplo, ascendente).
propiedad	prp.property: identificador que hace referencia al registro de la tabla prptpl. Representa la plantilla a partir de la que se ha creado la propiedad. prp.property=prptpl.code.
valor	prp.value: valor introducido por el usuario en respuesta a los campos prp_description y prp.label.
prp_last_mod_dt	prp.last_mod_dt: indicación de tiempo (pdmtime) que señala cuándo se modificó por última vez la propiedad.
prp_last_mod_by	prp.last_mod_by: identificador binario que hace referencia al registro de la tabla ca_contact. Representa la persona que ha modificado por última vez el registro. prp.last_mod_by = ca_contact.contact_uuid.
obligatorio	prp.required: valor booleano que indica si la propiedad debe tener algún valor prp.value para poder guardar el registro.
muestra	prp.sample: campo de texto que muestra valores de ejemplo que sirven al usuario para escribir el valor más útil en el campo prp.value.

Campo	Observaciones
prp_description	prp.description: campo de texto donde se explica el tipo de valor que se debe introducir en el campo prp.value.
etiqueta	prp.label: descripción breve del valor que se debe indicar en el campo prp.value.

View_Contact_Full

Los siguientes campos constituyen una vista básica de todos los contactos. En esta vista se presentan todos los campos de la tabla ca_contact además de algunos campos de referencia como los que atañen a la descripción breve del tipo de contacto, el nombre de la ubicación, el nombre de las organizaciones y el tipo de servicio de cada uno de los contactos. La vista se ha unido con las tablas ca_location, ca_organization, srv_desc y ca_contact_type para obtener los nombres y los símbolos reales de algunos de los campos de la tabla ca_contact. Dichos nombres y símbolos se sitúan al final de la lista de campos de la vista.

Campo	Observaciones
contact_uuid	ca_contact.contact_uuid: identificador exclusivo binario para cada registro de la tabla ca_contact.
middle_name	ca_contact.middle_name: segundo nombre del contacto.
alias	ca_contact.alias: nombre alternativo, a menudo informal, del contacto.
last_name	ca_contact.last_name: apellidos del contacto.
first_name	ca_contact.first_name: nombre del contacto.
pri_phone_number	ca_contact.pri_phone_number: número de teléfono principal del contacto.
alt_phone_number	ca_contact.alt_phone_number: número de teléfono alternativo del contacto.
fax_number	ca_contact.fax_number: número de fax del contacto.
mobile_phone	ca_contact.mobile_phone: número de teléfono móvil del contacto.
pager_number	ca_contact.pager_number: número al que se emiten los mensajes para el buscapersonas del contacto.
email_address	ca_contact.email_address: dirección de correo electrónico del contacto.
location_uuid	ca_contact.location_uuid: identificador exclusivo binario que

Campo	Observaciones
	hace referencia a un registro de la tabla ca_location, que indica la ubicación fija del contacto. ca_contact.location_uuid = ca_location.location_uuid.
floor_location	ca_contact.floor_location: número de piso del contacto.
pager_email_address	ca_contact.pager_email_address: dirección de correo electrónico del buscapersonas del contacto.
room_location	ca_contact.room_location: habitación específica del piso de la ubicación fija del contacto.
contact_type	ca_contact.contact_type: entero que es el identificador exclusivo que hace referencia a una fila de la tabla ca_contact_type y que indica la función general del contacto dentro de la aplicación Service Desk. ca_contact.contact_type = ca_contact_type.id.
inactive	ca_contact.inactive: indicador booleano del estado del registro que determina su inclusión en las búsquedas estándar en Service Desk o su exclusión de ellas.
creation_user	ca_contact.creation_user: ID de usuario del contacto que creó el registro. ca_contact.creation_user = ca_contact.userid.
creation_date	ca_contact.creation_date: indicación de tiempo (pdmtime) que señala la fecha y la hora en que se creó el contacto.
last_update_user	ca_contact.last_update_user: ID de usuario del contacto que actualizó por última vez el registro del contacto. ca_contact.last_update_user = ca_contact.userid.
last_update_date	ca_contact.last_update_date: indicación de tiempo (pdmtime) que señala la fecha y la hora en que se modificó por última vez el registro.
version_number	ca_contact.version number: indicador de versión interna.
departamento	ca_contact.department: entero que es el identificador exclusivo que hace referencia a una fila de la tabla ca_resource_department, que indica el departamento del contacto. ca_contact.department = ca_resource_department.id.
comentario	ca_contact.comment: campo de texto para un comentario de formato libre que sirve para que los analistas documenten hechos importantes que influyen en el tratamiento de este contacto en particular.
company_uuid	ca_contact.company_uuid: identificador exclusivo binario que hace referencia a una fila de la tabla ca_company. Indica la afiliación del contacto a una compañía.

Campo	Observaciones
	ca_contact.company_uuid = ca_company.company_uuid.
organization_uuid	ca_contact.organizaiton_uuid: identificador exclusivo binario que hace referencia a una fila de la tabla ca_organization. Indica la organización de trabajo del contacto. ca_contact.organizaiton_uuid = ca_organization.organization_uuid.
admin_organization_uuid	ca_contact.admin_organization_uuid: identificador exclusivo binario que hace referencia a una fila de la tabla ca_organization. Indica la organización administrativa del contacto. ca_contact.admin_organization_uuid = ca_organization.organization_uuid.
alternate_identifier	ca_contact.alternate_identifier: identificador definido por el usuario que suele ser una entidad empleada por el departamento de recursos humanos para identificar de forma exclusiva al contacto.
job_title	ca_contact.job_title: entero que es el identificador exclusivo que hace referencia a la tabla ca_job_title. Indica el título de trabajo normalizado del contacto. ca_contact.job_title = ca_job_title.id.
job_function	ca_contact.job_function: entero que es el identificador exclusivo que hace referencia a la tabla ca_job_function. Indica la descripción general normalizada de la función del trabajo del contacto. ca_contact.job_function = ca_job_function.id.
mail_stop	ca_contact.mail_stop: punto de distribución del correo.
cost_center	ca_contact.cost_center: entero que es el identificador exclusivo que hace referencia a la tabla ca_contact.cost_center. Indica el centro de costes principal del contacto. ca_contact.cost_center = ca_cost_center.id.
ID de usuario	ca_contact.userid: identificador de usuario que usa el contacto para iniciar sesión en Service Desk.
supervisor_contact_uuid	ca_contact.supervisor_contact_uuid: identificador exclusivo binario que hace referencia a una fila de la tabla ca_contact, que crea una jerarquía de contactos para indicar la estructura de informes de cada uno de los contactos. ca_contact.supervisor_contact_uuid = ca_contact.contact_uuid.
exclude_registration	ca_contact.exclude_registration: indicador interno.
delete_time	ca_contact.delete_time: indicación de tiempo que señala cuándo se estableció el indicador de inactividad en 1.
contact_type_name	ca_contact_type.name: descripción breve del valor

Campo	Observaciones
	ca_contact.contact_type del contacto.
location_name	ca_location.name: descripción breve de la ubicación fija del contacto.
organización	ca_organization.org_name: descripción breve del valor ca_contact.organization_uuid del contacto.
admin_organization	ca_organization.org_name: descripción breve del nombre de la organización del contacto. ca_contact.admin_organization_uuid.
service_type	srv_desc.sym: descripción breve del valor usp_contact.c_service_type del contacto. ca_contact.contact_uuid = usp_contact.contact_uuid Y usp_contact.c_service_type = srv_desc.code.
state_sym	ca_location.state: entero que es el identificador exclusivo que hace referencia a una fila de la tabla ca_state_province, que indica el estado, la provincia u otra región geográfica política. ca_contact.location_uuid = ca_location.location_uuid Y ca_location.state = ca_state_province.id.

View_Contact_to_Environment

La siguiente lista de campos es una vista básica de los contactos y su entorno (activos). Presenta la vista de la tabla de contactos (ca_contact), que se une con la tabla de recursos de propiedad (ca_owned_resource) para obtener una lista de todos los activos asociados a los contactos. Se puede unir esta vista con la vista View_Contact_Full a fin de obtener el tipo de contacto, el tipo de servicio, las organizaciones y la ubicación que correspondan a cada uno de los contactos. Para obtener dicha información, también cabe la posibilidad de unirla con cada una de las tablas pertinentes.

Campo	Observaciones
ca_contact.*	Campos de la tabla ca_contact indicados en la definición de la vista View_Contact_Full.
asset_uuid	ca_owned_resource.own_resource_uuid: identificador exclusivo binario para cada activo de la tabla ca_owned_resource.
asset_name	ca_owned_resource.resource_name: nombre de red designado para el activo.

View_Group

La siguiente lista de campos es una vista básica de la tabla de contactos, pero sólo muestra los contactos del grupo. El ID de tipo de contacto es 2308, que es el destinado a los tipos de grupos. Si se desean obtener datos más significativos para la generación de informes, es posible unir esta vista con otras tablas de CA Service Desk Manager. Por ejemplo, puede unirla con la tabla de ubicaciones (ca_location) para buscar el nombre y la dirección de la ubicación del grupo. También puede unir esta vista con la tabla de organizaciones (ca_organization) para obtener los nombres de las organizaciones funcional y administrativa del grupo.

Campo	Observaciones
ca_contact.*	Campos de la tabla ca_contact indicados en la definición de la vista View_Group_Full.

El siguiente ejemplo muestra cómo funciona la unión de tablas y cómo se extraen los campos para los informes. El campo de una tabla (la de la derecha) se une (->) con el campo de otra tabla (la de la izquierda). A fin de realizar la adecuada unión de las tablas y las vistas, es preciso comprender las diferencias de las uniones de las bases de datos. Tal como se ilustra a continuación, el campo definido entre paréntesis es el que puede ser conveniente emplear en los informes si se han unido las tablas anteriores con la vista View_Group:

- View_Group.contact_type -> ca_contact_type.id (ca_contact_type.sym)
- View_Group.location_uuid -> ca_location.location_uuid (ca_location.location_name)
- View_Group.organization_uuid -> ca_organization.organization_uuid (ca_organization.org_name)
- View_Group.admin_organization_uuid -> ca_organization(2).organization_uuid (ca_organization(2). org_name)

View_Group_To_Contact

La siguiente lista de campos es una vista básica de todos los contactos del grupo (miembros). que incluye, asimismo, a los gestores. En ella se une la vista View_Group con la tabla Group_Member y, a continuación, con la tabla ca_contact. Se muestran todos los campos de la vista View_Group, además de los campos del nombre, del segundo nombre y de los apellidos que figuren en la tabla ca_contact. También se muestra el indicador de gestor de Group_Member, cuyos valores son 1 y 0: 1 (sí) significa que se trata de un gestor y 0 (no), que no lo es. La mayor parte de la información de esta vista atañe al grupo en sí, no a sus miembros. La vista sirve para buscar información sobre un grupo en particular, incluidos los nombres de sus miembros.

Campo	Observaciones
View_Group.*	Campos View_Group indicados en la definición de View_Group.
member_lastname	ca_contact.last_name: apellidos del miembro del grupo.
member_firstname	ca_contact.first_name: nombre del miembro del grupo.
member_middlename	ca_contact.middle_name: segundo nombre del miembro del grupo.
grpmem_manager_flag	ca_contact.manager_flag: indicador del gestor de miembros del grupo (1 o 0).

View_Issue

Se trata de una vista básica de todas las incidencias donde figuran datos como el estado, la prioridad, la categoría, las organizaciones, el nombre completo del solicitante, el nombre completo del asignatario, el nombre del grupo, el ID del grupo, etc. En ella se une la tabla issue con muchas otras tablas a fin de obtener datos más significativos sobre las incidencias.

Campo	Observaciones
ID	issue.id: identificador exclusivo para el registro en la tabla issue.
persid	issue.persid: identificador exclusivo para el registro en la tabla issue precedido por el identificador de objeto (iss para la tabla issue) y dos puntos.
issue_ref_num	issue.iss_ref_num: número de referencia de la incidencia que emplean los analistas y los clientes para hacer referencia a ella en particular.

Campo	Observaciones
descripción	issue.description: descripción completa de la incidencia redactada por un analista o un cliente.
estado	issue.status: identificador exclusivo del estado de la incidencia, que es un puntero a la tabla issstat. issue.status = issstat.code.
active_flag	issue.active_flag: indicador entero que determina si la incidencia está activa o no (1 ó 0).
start_date	issue.start_date: fecha en la que la tarea pasa por primera vez al estado pendiente (pdmtime).
open_date	issue.open_date: fecha de creación de la incidencia (pdmtime).
last_mod_dt	issue.last_mod_dt: fecha de la última modificación (pdmtime).
last_mod_by	issue.last_mod_by: puntero al UUID del contacto que ha modificado por última vez la incidencia. issue.last_mod_by = ca_contact.contact_uuid.
close_date	issue.close_date: fecha en la que se ha definido la incidencia como inactiva (pdmtime).
resolve_date	issue.resolve_date: fecha en la que se ha definido la incidencia en un estado configurado para indicar que la incidencia se ha resuelto (pdmtime).
rootcause	issue.rootcause: puntero al registro de la tabla rootcause que representa la situación original que exigía el registro de la incidencia. issue.rootcause = rootcause.id.
est_total_time	issue.est_total_time: tiempo total estimado (pdmtime) para finalizar la incidencia.
actual_total_time	issue.actual_total_time: tiempo total (pdmtime) que se ha tardado en finalizar la incidencia.
log_agent	issue.log_agent: identificador exclusivo binario que hace referencia a la tabla ca_contact, que a la vez hace referencia a la persona que es el creador original de la incidencia. issue.log_agent = ca_contact.contact_uuid.
asignado	issue.assignee: puntero al UUID del contacto que está asignado actualmente a la orden de cambio. issue.assignee = ca_contact.contact_uuid.
organización	issue.organization: puntero al UUID de la organización interna que representa la organización a la que pertenece la incidencia. issue.organization = ca_organization.organization_uuid.
group_id	issue.group_id: puntero al UUID del contacto que representa el grupo que está asignado actualmente a la incidencia. issue.group_id = ca_contact.contact_uuid.

Campo	Observaciones
affected_contact	issue.affected_contact: puntero al UUID del contacto que representa el contacto afectado por la incidencia. issue.affected_contact = ca_contact.contact_uuid.
solicitante	issue.requestor: puntero al UUID del contacto que representa la persona que ha solicitado el registro de la incidencia. issue.requestor = ca_contact.contact_uuid.
categoría	issue.category: puntero al código de la categoría de incidencias para obtener la categoría en la que entra la incidencia. issue.category = isscat.code.
prioridad	issue.priority: puntero al valor de prioridad que representa la prioridad en la que entra la incidencia. issue.priority = pri.enum.
need_by	issue.need_by: fecha que indica para cuándo necesita el usuario affected_end_user tener finalizada la incidencia (pdmtime).
est_comp_date	issue.est_comp_date: fecha de finalización estimada (pdmtime) de la incidencia.
actual_comp_date	issue.actual_comp_date: fecha de finalización real (pdmtime) de la incidencia.
est_cost	issue.est_cost: coste estimado de la incidencia.
actual_cost	issue.actual_cost: coste real de la implementación de la incidencia.
justificación	issue.justification: campo de texto para que el solicitante documente los motivos por los que se precisa la incidencia.
backout_plan	issue.backout_plan: campo de texto para que el analista documente el plan de retroceso de la incidencia.
impact	issue.impact: puntero al registro de la tabla impact que indica el ámbito de los recursos a los que afecta la incidencia. issue.impact = impact.enum.
principal	issue.parent: puntero al ID de otra incidencia que permite la creación de una jerarquía de incidencias. issue.parent = issue.id.
dificultad	issue.effort: campo de texto para explicar el plan de implementación de la incidencia.
support_lev	issue.support_lev: puntero a un registro de descripción del servicio que automatiza algunas de las restricciones para las que se debe finalizar la incidencia. issue.support_lev = srv_desc.code.
template_name	issue.template_name: nombre de la plantilla de la incidencia y puntero a la misma. issue.template_name = iss_template.template_name.

Campo	Observaciones
sla_violation	issue.sla_violation: entero que representa el número de veces que se ha infringido el acuerdo de nivel de servicio adjunto a la incidencia.
predicted_sla_viol	issue.predicted_sla_viol (r5.5): campo destinado a la tecnología relacionada con Neugent.
macro_predict_viol	issue.macro_predict_viol (r5.5): campo destinado a la tecnología relacionada con Neugent.
created_via	issue.created_via: puntero a un registro de la tabla interface. Indica en qué interfaz se ha originado la incidencia. issue.created_via = interface.id.
call_back_date	issue.call_back_date: campo de fecha y hora (pdmtime) que indica la fecha y la hora futuras en que hay que ponerse en contacto con el solicitante.
call_back_flag	issue.call_back_flag: indicador booleano que se presenta como una casilla de verificación al usuario y que indica si hay que enviar una notificación al analista en la fecha de issue.call_back_date.
string1	Campo de texto susceptible de definición por parte del usuario.
string2	Campo de texto susceptible de definición por parte del usuario.
string3	Campo de texto susceptible de definición por parte del usuario.
string4	Campo de texto susceptible de definición por parte del usuario.
string5	Campo de texto susceptible de definición por parte del usuario.
string6	Campo de texto susceptible de definición por parte del usuario.
service_date	issue.service_date: fecha y hora (pdmtime) cuando se prevé que el distribuidor externo atienda la incidencia.
service_num	issue.service_num: campo de texto para documentar el número del pedido de compra o la orden de servicio del distribuidor externo.
producto	issue.product: puntero al registro de la tabla product que indica el producto al que afecta la incidencia. issue.product = product.id.
acciones	issue.actions: campo de texto de gran tamaño para documentar las acciones.
type_of_contact	issue.type_of_contact: puntero al registro de la tabla toc que indica la categorización general de la perspectiva del usuario affected_end_user de la incidencia. issue.type_of_contact = toc.id.
reporting_method	issue.reporting_method: puntero al registro de la tabla repmeth que clasifica el origen de la incidencia y que selecciona la persona que crea la incidencia. issue.reporting_method = repmeth.id.

Campo	Observaciones
person_contacting	issue.person_contacting: puntero al registro de la tabla perscon que indica el rol de los usuarios affected_end_user o requestor. issue.person_contacting = perscon.id.
status_name	issstat.sym: descripción del estado como lo ve el usuario. issue.status = issstat.code.
priority_num	pri.sym: descripción de la prioridad como la ve el usuario. issue.priority = pri.enum.
category_name	isscat.sym: nombre de la categoría de incidencias como la ve el usuario. issue.category = isscat.code.
organization_name	ca_organization.org_name: nombre de la organización como lo ve el usuario. issue.organization = ca_organization.organization_uuid.
affected_end_user_lastname	ca_contact.last_name: apellidos del usuario final afectado. issue.affected_end_user = ca_contact.contact_uuid.
affected_end_user_firstname	ca_contact.first_name: nombre del usuario final afectado. issue.affected_end_user = ca_contact.contact_uuid.
affected_end_user_middlename	ca_contact.middle_name: segundo nombre del usuario final afectado. issue.affected_end_user = ca_contact.contact_uuid.
assignee_lastname	ca_contact.last_name: apellidos del asignatario. issue.assignee = ca_contact.contact_uuid.
assignee_firstname	ca_contact.first_name: nombre del asignatario. issue.assignee = ca_contact.contact_uuid.
assignee_middlename	ca_contact.middle_name: segundo nombre del asignatario. issue.assignee = ca_contact.contact_uuid.
groupID	View_Group.contact_uuid: representación binaria del ID interno empleado para el grupo asignado a la incidencia. issue.group_id = ca_contact.contact_uuid.
group_name	View_Group.last_name: nombre del grupo asignado a la incidencia. issue.group = ca_contact.contact_uuid.
service_type	srv_desc.sym: nombre del tipo de servicio aplicado a la incidencia. issue.support_lev = srv_desc.code.
impact_num	impact.sym: descripción del impacto como lo ve el usuario. issue.impact = impact.enum.
product_sym	product.sym: descripción del producto como lo ve el usuario. issue.product = product.id.
type_of_contact_sym	toc.sym: descripción del tipo de contacto como lo ve el usuario. issue.type_of_contact = toc.id.

Campo	Observaciones
rpting_method_sym	repmeth.sym: descripción del método de presentación de informes como lo ve el usuario. issue.reporting_method = repmeth.id.
person_contacting_sym	perscon.sym: descripción de la persona de contacto como la ve el usuario. issue.person_contacting = perscon.id.
created_via_sym	interface.sym: issue.created_via = interface.id.
rootcause_sym	rootcause.sym: issue.rootcause = rootcause.id.

View_Issue_Act_Log

Se trata de una vista básica de todos los registros de actividades de las incidencias. Esta vista aúna la tabla del registro de actividades de incidencias (issalg) y las tablas del tipo de actividad (act_type) y de contactos (ca_contact) para obtener datos más significativos como, por ejemplo, el tipo de actividad real y el nombre completo del analista que ha llevado a cabo la actividad.

Campo	Observaciones
ID	issalg.id: identificador exclusivo para el registro en la tabla issalg.
persid	issalg.persid: identificador exclusivo para el registro en la tabla issalg precedido por el identificador de objeto (issalg para la tabla issalg) y dos puntos.
issue_id	issalg.issue_id: puntero al ID de la incidencia a la que pertenece la actividad. issalg.issue_id = issalg.id.
last_mod_dt	issalg.last_mod_dt: fecha y hora de la última modificación (pdmtime).
time_spent	issalg.time_spent: tiempo empleado en la actividad, almacenado como el número total de segundos. por ejemplo, 80 = 1 minuto y 20 segundos.
time_stamp	issalg.time_stamp: fecha y hora de la actividad susceptible de modificación por el usuario (pdmtime).
system_time	issalg.system_time: fecha y hora de creación del registro (pdmtime).
analista	issalg.analyst: identificador exclusivo binario que hace referencia al UUID del contacto para obtener el analista que realizó la actividad. issalg.analyst = ca_contact.contact_uuid.

Campo	Observaciones
descripción	issalg.description: texto descriptivo de la actividad susceptible de modificación por parte del usuario.
action_desc	issalg.action_desc: texto descriptivo de la acción automatizada que no es susceptible de modificación por parte del usuario.
tipo	issalg.type: puntero de texto a un registro de la tabla de tipos de actividades. issalg.type = act_type.code.
interno	issalg.internal: indicador en forma de entero (1 ó 0), que señala si la entrada del registro pueden consultarla todos los usuarios o sólo es para uso interno.
knowledge_session	issalg.knowledge_session: identificador de una sesión en particular de un usuario concreto.
knowledge_tool	issalg.knowledge_tool: indicador de la herramienta de conocimiento empleada para la búsqueda como, por ejemplo, NLS_FAQ, EXPERT, etc.
analyst_lastname	View_Contact_Full.last_name: apellidos del analista derivados de issalg.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: nombre del analista.
analyst_middlename	View_Contact_Full.middle_name: segundo nombre del analista.
activity_type	act_type.sym: tipo de actividad al que hace referencia issalg.type = act_type.code.

View_Issue_to_Assets

La siguiente lista de campos es una vista básica de las incidencias y sus activos. La tabla de incidencias (issue) se une de forma indirecta con la tabla de recursos de propiedad (ca_owned_resource) y otras tablas relacionadas con los activos para obtener una lista de los activos de las incidencias. Es posible que no figuren todas las incidencias, en particular si no disponen de activos.

Campo	Observaciones
View_Issue.*	Vista View_Issue que define todos los campos que aparecen en la vista de View_Issue.
assetID	ca_owned_resource.own_resource_uuid: campo binario que actúa como identificador exclusivo interno que no cambia para el registro del activo.
asset_serial_num	ca_owned_resource.serial_number: número de serie del registro del

Campo	Observaciones
	activo.
asset_class	ca_resource_class.name: descripción breve de la clase a la que pertenece el activo. ca_owned_resource.resource_class = ca_resource_class.id.
asset_family	ca_resource_family.name: familia de activos a la que pertenece el activo. ca_owned_resource.resource_class = ca_resource_class.id Y ca_resource_class.family_id = ca_resource_family.id.
asset_name	ca_owned_resource.resource_name: nombre de red por el que se conoce el activo.

View_Issue_to_Issue_Act_Log

Se trata de una vista básica de todas las incidencias y de los registros de actividades que las acompañan. Esta vista aúna la vista View_Issue y la vista View_Issue_Act_Log para ofrecer información detallada sobre las incidencias y sus registros de actividades. Los datos reales se sitúan al final de la lista de campos.

Campo	Observaciones
View_Issue.*	Campos indicados en la definición anterior de la vista View_Issue de este documento.
issalg_id	issalg.id: identificador exclusivo para el registro en la tabla issalg.
issalg_persid	issalg.persid: identificador exclusivo para el registro en la tabla issalg precedido por el identificador de objeto (issalg para la tabla issalg) y dos puntos.
issue_id	issalg.issue_id: puntero al ID de la incidencia a la que pertenece la actividad. issalg.issue_id = issalg.id.
issalg_last_mod_dt	issalg.last_mod_dt: fecha y hora de la última modificación (pdmtime).
time_spent	issalg.time_spent: tiempo empleado en la actividad, almacenado como el número total de segundos. por ejemplo, 80 = 1 minuto y 20 segundos.
time_stamp	issalg.time_stamp: fecha y hora de la actividad susceptible de modificación por el usuario (pdmtime).

Campo	Observaciones
system_time	issalg.system_time: fecha y hora de creación del registro (pdmtime).
analista	issalg.analyst: puntero binario exclusivo al UUID del contacto para obtener el analista que realizó la actividad. issalg.analyst = ca_contact.contact_uuid.
issalg_description	issalg.description: texto descriptivo de la actividad susceptible de modificación por parte del usuario.
action_desc	issalg.action_desc: texto descriptivo de la acción automatizada que no es susceptible de modificación por parte del usuario.
tipo	issalg.type: puntero de texto a un registro de la tabla de tipos de actividades. issalg.type = act_type.code.
interno	issalg.internal: indicador en forma de entero (1 ó 0), que señala si la entrada del registro pueden consultarla todos los usuarios o sólo es para uso interno.
knowledge_session	issalg.knowledge_session: identificador de una sesión en particular de un usuario concreto.
knowledge_tool	issalg.knowledge_tool: indicador de la herramienta de conocimiento empleada para la búsqueda como, por ejemplo, NLS_FAQ, EXPERT, etc.
issalg_analyst_id	issalg.analyst: puntero binario exclusivo al UUID del contacto para obtener el analista que realizó la actividad. issalg.analyst = ca_contact.contact_uuid.

View_Change_to_Requests

Se trata de una vista básica sólo de las órdenes de cambios que tienen asignadas solicitudes. Esta vista es el resultado de unir la vista View_Change y la tabla de solicitudes (call_req) para ofrecer detalles relativos a las órdenes de cambio y sus solicitudes asociadas.

Campo	Observaciones
View_Change.*	Muestra todos los campos antes enumerados para la vista View_Change.
cr_id	call_req.id: identificador exclusivo para el registro en la tabla call_req.

Campo	Observaciones
ref_num	call_req.ref_num: número de referencia de la solicitud que emplean los analistas y los clientes para hacer referencia a una solicitud en particular.
cr_summary	call_req.summary: descripción breve de la solicitud para la consulta rápida.
cr_persid	call_req.persid: identificador exclusivo para el registro en la tabla call_req precedido por el identificador del objeto (cr para la tabla call_req) y dos puntos.
cr_description	call_req.description: descripción completa de la solicitud redactada por un analista o un cliente.
cr_status	call_req.status: identificador exclusivo que hace referencia al registro de la tabla cr_stat. Indica el estado de la solicitud: call_req.status = cr_stat.code
cr_active_flag	call_req.active_flag: indicador en forma de entero que determina si el registro de la solicitud está activo o no (1 o 0).
time_spent_sum	call_req.time_spent_sum: total derivado de todos los campos time_spent de los registros de la tabla act_log almacenados en segundos (por ejemplo, 80 = 1 minuto y 20 segundos).
cr_open_date	call_req.open_date: sello de hora de la creación de la solicitud (pdmtime).
cr_last_mod_dt	call_req.last_mod_dt: sello de hora de la última modificación (pdmtime).
cr_close_date	call_req.close_date: indicación de tiempo en la que se estableció la solicitud como inactiva (pdmtime).
cr_log_agent	call_req.log_agent: identificador exclusivo binario que hace referencia a la tabla ca_contact. Hace referencia a la persona de la tabla que es el creador original de la solicitud. call_req.log_agent = ca_contact.contact_uuid.
cr_group_id	call_req.group_id: identificador exclusivo binario que hace referencia a un registro de la tabla ca_contact. Representa el grupo que está asignado actualmente a la solicitud. call_req.group_id = ca_contact.contact_uuid.
cr_assignee	call_req.assignee: identificador exclusivo binario que hace referencia a un registro de la tabla ca_contact. Representa la persona que está asignada actualmente a la solicitud. call_req.assignee = ca_contact.contact_uuid.
cliente	call_req.customer: identificador exclusivo binario que hace referencia a un registro de la tabla ca_contact. Representa el usuario final afectado por la solicitud. call_req.customer = ca_contact.contact_uuid.

Campo	Observaciones
charge_back_id	charge_back_id: campo de texto disponible para su uso como indicador en jerga contable para cargar la solicitud al centro de costes adecuado.
affected_rc	call_req.affected_rc: identificador exclusivo binario que hace referencia a una fila de la tabla ca_owned_resource. Representa el activo al que se aplica la solicitud. call_req.affected_rc = ca_owned_resource.own_resource_uuid.
cr_support_lev	call_req.support_lev: puntero a un registro de descripción del servicio que automatiza algunas de las restricciones para las que se debe finalizar la solicitud. call_req.support_lev = srv_desc.code
cr_category	call_req.category: identificador exclusivo que hace referencia al registro de la tabla prob_ctg. Representa la categoría a la que pertenece la solicitud. call_req.category = prob_ctg.persid
solución	call_req.solution: puntero a la solución de la llamada para obtener la solución. call_req.solution = crsol.persid.
cr_impact	call_req.impact: entero que es el identificador exclusivo que hace referencia a una fila de la tabla impact. Indica el ámbito al que afecta la solicitud. call_req.impact = impact.enum.
cr_priority	call_req.priority: entero que es el identificador exclusivo que hace referencia a un registro de la tabla pri. Indica el modo en el que los analistas priorizan el trabajo asociado a la solicitud. call_req.priority = pri.enum
urgencia	call_req.urgency: entero que es el identificador exclusivo que hace referencia a una fila de la tabla urgency. Documenta el grado de urgencia según el usuario con el que se debe resolver la solicitud. call_req.urgency = urgncy.enum
gravedad	call_req.severity: entero que es el identificador exclusivo que hace referencia a una fila de la tabla severity. Indica la gravedad de las consecuencias si no se resuelve la solicitud. call_req.severity = sevrty.enum
extern_ref	Parte asociado.
last_act_id	ID de la última actividad.
cr_ticket	Puntero al parte de incidencia para obtener el parte asociado.
cr_parent	call_req.parent: puntero de ID persistente al ID persistente de otra solicitud que facilita la creación de una jerarquía de órdenes de cambio.

Campo	Observaciones
	call_req.parent = call_req.persid.
cr_template_name	call_req.template_name: valor de texto que indica la designación de la solicitud para su elegibilidad de una lista como plantilla para solicitudes similares. cr_template.template = call_req.persid.
cr_sla_violation	call_req.sla_violation: entero que representa el recuento de veces que se han infringido los acuerdos de nivel de servicio adjuntos a la solicitud.
cr_predicted_sla_viol	call_req.predicted_sla_viol (r5.5): campo destinado a la tecnología relacionada con Neugent.
cr_created_via	call_req.created_via: entero que es el puntero al registro de la tabla interface. Indica en qué interfaz se ha originado la orden de cambios. call_req.created_via = interface.id.
cr_call_back_date	call_req.call_back_date: campo de indicación de tiempo (pdmtime) que señala la fecha y la hora futuras cuando hay que ponerse en contacto con el usuario affected_end_user.
cr_call_back_flag	call_req.call_back_flag: indicador booleano que se presenta al usuario como casilla de verificación y que indica si hay que enviar una notificación al analista en la fecha de call_req.call_back_date.
event_token	call_req.event_token: valor que emplea CA NSM para el cotejo de mensajes.
tipo	call_req.type: campo de texto que hace referencia a un registro de la tabla crt. Indica el tipo ITIL de la solicitud. call_req.type = crt.code
cr_string1	Cadena susceptible de definición por parte del usuario.
cr_string2	Cadena susceptible de definición por parte del usuario.
cr_string3	Cadena susceptible de definición por parte del usuario.
cr_string4	Cadena susceptible de definición por parte del usuario.
cr_string5	Cadena susceptible de definición por parte del usuario.
cr_string6	Cadena susceptible de definición por parte del usuario.
cambiar	call_req.change: entero que es el identificador exclusivo que hace referencia a una fila de la tabla chg. Indica la orden de cambios creada como resultado de la solicitud. call_req.change = chg.id.

View_Issue_to_Issue_WF

Esta vista es el resultado de aunar la vista View_Issue y la tabla de tareas de workflow (isswf) para ofrecer una vista básica de las incidencias y sus tareas de workflow. Es posible que no figuren todas las incidencias, en particular si no tienen asignada ninguna tarea de workflow.

Campo	Observaciones
View_Issue.*	Campos indicados en la definición anterior de la vista View_Issue de este documento.
wf_id	isswf.id: identificador exclusivo para el registro en la tabla isswf.
wf_persid	isswf.persid: identificador exclusivo para el registro en la tabla isswf, precedido por el identificador de objeto (isswf) y dos puntos.
del	isswf.del: indicador booleano que señala si el registro se debe mostrar al usuario.
object_type	isswf.object_type: nombre de fábrica empleado para identificar el tipo de registro (por ejemplo, iss) al que se adjunta esta tarea de workflow.
object_id	isswf.object_id: identificador exclusivo empleado para identificar el registro específico al que se adjunta esta tarea de workflow. isswf.object_id = issue.id.
tarea	isswf.task: identificador que hace referencia al tipo de tarea que representa el registro. isswf.task = tsqty.code.
wf_template	isswf.wf_template: identificador que hace referencia a la plantilla a partir de la que se creó el registro de la tarea de workflow. isswf.wf_template = wftpl.id.
secuencia	isswf.sequence: entero que indica el orden en el que CA Service Desk Manager debe mostrar y ejecutar el registro de esta tarea de workflow en particular (por, ejemplo, ascendente).
wf_status	isswf.status: identificador que hace referencia al registro tsqstat. Indica el estado actual de la tarea de workflow. isswf.status = tsqstat.code.
group_task	isswf.group_task: valor booleano que indica si la tarea pertenece a algún grupo.
activo	isswf.asset: identificador UUID (binario) que hace referencia a un registro de la tabla ca_owned_resource. isswf.asset = ca_owned_resource.own_resource_uuid.
creador	isswf.creator: identificador exclusivo binario que hace referencia a un registro de la tabla ca_contact. Indica la persona que ha creado la tarea de workflow.

Campo	Observaciones
	isswf.creator = ca_contact.contact_uuid.
date_created	isswf.date_created: fecha o indicación de tiempo que señala cuándo se creó la tarea de workflow (pdmtime).
wf_assignee	isswf.assignee: identificador exclusivo binario que hace referencia a un registro de la tabla ca_contact. Indica la persona que está asignada actualmente a la tarea de workflow. isswf.assignee = ca_contact.contact_uuid.
done_by	isswf.done_by: identificador exclusivo binario que hace referencia a un registro de la tabla ca_contact. Indica la persona que ha finalizado o aprobado la tarea de workflow. isswf.done_by = ca_contact.contact_uuid.
wf_start_date	wf_start_date: sello de hora que indica cuándo se ha movido la tarea de workflow a un estado activo (pdmtime).
wf_est_comp_date	isswf.est_comp_date: indicación de tiempo (pdmtime) que señala cuándo cree el usuario que estará finalizada la tarea.
est_duration	isswf.est_duration: duración estimada de la tarea de workflow.
completion_date	isswf.completion_date: indicación de tiempo (pdmtime) que señala cuándo se finalizó la tarea de workflow.
actual_duration	isswf.actual_duration: tiempo real que se tardó en finalizar la tarea de workflow.
wf_est_cost	isswf.est_cost: coste estimado de la tarea de workflow.
coste	isswf.cost: coste real necesario para finalizar la tarea de workflow.
wf_description	isswf.description: descripción de la tarea de workflow.

Campo	Observaciones
wf_last_mod_dt	isswf.last_mod_dt: indicación de tiempo (pdmtime) que señala cuándo se modificó por última vez la tarea de workflow.
wf_last_mod_by	isswf.last_mod_by: identificador exclusivo binario que hace referencia a un registro de la tabla de contacto. Indica la última persona que ha realizado algún cambio en la tarea de workflow. isswf.last_mod_by = ca_contact.contact_uuid.

View_Issue_to_Properties

Esta vista es el resultado de aunar la vista View_Issue y la tabla de propiedades de las incidencias (issprp) para ofrecer una vista básica de las incidencias y sus propiedades asignadas. Es posible que no figuren todas las incidencias, en particular si no tienen asignada ninguna propiedad.

Campo	Observaciones
View_Issue.*	Campos indicados en la definición anterior de la vista View_Issue de este documento.
prp_id	issprp.id: entero que es el identificador exclusivo para el registro de la propiedad.
prp_persid	issprp.persid: identificador exclusivo para el registro en la tabla prp, precedido por el identificador de objeto (prp) y dos puntos.
secuencia	issprp.sequence: entero que indica el orden en el que CA Service Desk Manager debe mostrar el registro de esta propiedad en particular (por, ejemplo, ascendente).
etiqueta	issprp.label: descripción breve del valor que se debe indicar en el campo issprp.value.
valor	issprp.value: valor introducido por el usuario en respuesta a los campos prp_description y issprp.label.
prp_last_mod_dt	issprp.last_mod_dt: indicación de tiempo (pdmtime) que indica cuándo se modificó por última vez la propiedad.
prp_last_mod_by	issprp.last_mod_by: identificador binario que hace referencia a un registro de la tabla ca_contact. Representa la persona que ha modificado por última vez el registro. issprp.last_mod_by = ca_contact.contact_uuid.
obligatorio	issprp.required: valor booleano que indica si la propiedad debe tener algún valor issprp.value para poder guardar el registro.

Campo	Observaciones
muestra	issprp.sample: campo de texto que muestra valores de ejemplo que sirven al usuario para introducir el valor más útil en el campo issprp.value.
owning_iss	issprp.owning_iss: identificador exclusivo empleado para identificar el registro específico al que se adjunta la propiedad. issprp.object_id = issue.persid.
prp_description	issprp.description: campo de texto donde se explica el tipo de valor que se debe introducir en el campo issprp.value.

View_Request

Se trata de una vista básica de todas las solicitudes. En ella se une la tabla de solicitudes con otras tablas de CA Service Desk Manager a fin de obtener información más específica como, por ejemplo, el tipo de servicio, la gravedad, la urgencia, la categoría o la prioridad de las solicitudes, además de algunos otros datos sobre éstas. Se seleccionan todos los campos de la tabla de solicitudes (call_req). Al final de la lista de campos aparecen los campos extraídos, que son el resultado de la unión de las tablas.

Campo	Observaciones
ID	call_req.id: identificador exclusivo para el registro en la tabla call_req.
persid	call_req.persid: identificador exclusivo para el registro en la tabla call_req precedido por el identificador del objeto (cr para la tabla call_req) y dos puntos.
ref_num	call_req.ref_num: número de referencia de la solicitud que emplean los analistas y los clientes para hacer referencia a una solicitud en particular.
resumen	call_req.summary: descripción breve de la solicitud para la consulta rápida.
descripción	call_req.description: descripción completa de la solicitud redactada por un analista o un cliente.
estado	call_req.status: identificador exclusivo que hace referencia al registro de la tabla cr_stat. Indica el estado de la solicitud. call_req.status = cr_stat.code
active_flag	call_req.active_flag: indicador en forma de entero que determina si el registro de la solicitud está activo o no (1 o 0).

Campo	Observaciones
open_date	call_req.open_date: sello de hora de la creación de la solicitud (pdmtime).
time_spent_sum	call_req.time_spent_sum: total derivado de todos los campos time_spent de los registros de la tabla act_log almacenados en segundos (por ejemplo, 80 = 1 minuto y 20 segundos).
last_mod_dt	call_req.last_mod_dt: sello de hora de la última modificación (pdmtime).
close_date	call_req.close_date: indicación de tiempo en la que se estableció la solicitud como inactiva (pdmtime).
resolve_date	fecha en la que se ha resuelto la solicitud (pdmtime).
rootcause	Puntero a rootcause.id.
log_agent	call_req.log_agent: identificador exclusivo binario que hace referencia a la tabla ca_contact. Hace referencia a la persona de la tabla que es el creador original de la solicitud. call_req.log_agent = ca_contact.contact_uid.
asignado	call_req.assignee: identificador exclusivo binario que hace referencia a un registro de la tabla ca_contact. Representa la persona que está asignada actualmente a la solicitud. call_req.assignee = ca_contact.contact_uid.
group_id	call_req.group_id: identificador exclusivo binario que hace referencia a un registro de la tabla ca_contact. Representa el grupo que está asignado actualmente a la solicitud. call_req.group_id = ca_contact.contact_uid.
cliente	call_req.customer: identificador exclusivo binario que hace referencia a un registro de la tabla ca_contact. Representa el usuario final afectado por la solicitud. call_req.customer = ca_contact.contact_uid.
charge_back_id	charge_back_id: campo de texto disponible para su uso como indicador en jerga contable para cargar la solicitud al centro de costes adecuado.
affected_rc	call_req.affected_rc: identificador exclusivo binario que hace referencia a una fila de la tabla ca_owned_resource. Representa el activo al que se aplica la solicitud. call_req.affected_rc = ca_owned_resource.own_resource_uid.

Campo	Observaciones
support_lev	call_req.support_lev: puntero a un registro de descripción del servicio que automatiza algunas de las restricciones para las que se debe finalizar la solicitud. call_req.support_lev = srv_desc.code.
categoría	call_req.category: identificador exclusivo que hace referencia a un registro de la tabla prob_ctg. Representa la categoría a la que pertenece la solicitud. call_req.category = prob_ctg.persid
solución	call_req.solution: puntero a la solución de la llamada para obtener la solución. call_req.solution = crsol.persid.
impact	call_req.impact: entero que es el identificador exclusivo que hace referencia a una fila de la tabla impact. Indica el ámbito de impacto de la solicitud. call_req.impact = impact.enum.
prioridad	call_req.priority: entero que es el identificador exclusivo que hace referencia a un registro de la tabla pri. Indica el modo en el que los analistas priorizan el trabajo asociado a la solicitud. call_req.priority = pri.enum
urgencia	call_req.urgency: entero que es el identificador exclusivo que hace referencia a una fila de la tabla urgency. Indica el grado de urgencia según el usuario con el que se debe resolver la solicitud. call_req.urgency = urgncy.enum
gravedad	call_req.severity: entero que es el identificador exclusivo que hace referencia a una fila de la tabla severity. Indica la gravedad de las consecuencias si no se resuelve la solicitud. call_req.severity = sevrty.enum
extern_ref	Referencia externa a un parte asociado.
last_act_id	ID de la última actividad.
cr_ticket	Puntero al parte de incidencia para obtener el parte asociado.
principal	call_req.parent: puntero de ID persistente al ID persistente de otra solicitud que facilita la creación de una jerarquía de órdenes de cambio. call_req.parent = call_req.persid.

Campo	Observaciones
template_name	call_req.template_name: valor de texto que indica la designación de la solicitud para su elegibilidad de una lista como plantilla para solicitudes similares. cr_template.template = call_req.persid.
sla_violation	call_req.sla_violation: entero que representa el recuento de veces que se han infringido los acuerdos de nivel de servicio adjuntos a la solicitud.
predicted_sla_viol	Solicitud que es probable que infrinja el acuerdo de nivel de servicio, según las previsiones de Neugent.
macro_predicted_violation	Solicitud que es probable que infrinja el acuerdo de nivel de servicio, según las previsiones de Neugent.
created_via	call_req.created_via: entero que es el puntero al registro de la tabla interface que indica en qué interfaz se originó la orden de cambio. call_req.created_via = interface.id.
call_back_date	call_req.call_back_date: campo de indicación de tiempo (pdmtime) que señala la fecha y la hora futuras cuando hay que ponerse en contacto con el usuario affected_end_user.
call_back_flag	call_req.call_back_flag: indicador booleano que se presenta al usuario como casilla de verificación y que indica si hay que enviar una notificación al analista en la fecha de call_req.call_back_date.
event_token	call_req.event_token: valor que emplea CA NSM para el cotejo de mensajes.
sched_token	call_req.sched_token: valor que emplea CA NSM para el cotejo de mensajes.
tipo	call_req.type: campo de texto que hace referencia a un registro de la tabla crt. Indica el tipo ITIL de la solicitud. call_req.type = crt.code
string1	Cadena susceptible de definición por parte del usuario.
string2	Cadena susceptible de definición por parte del usuario.
string3	Cadena susceptible de definición por parte del usuario.

Campo	Observaciones
string4	Cadena susceptible de definición por parte del usuario.
string5	Cadena susceptible de definición por parte del usuario.
string6	Cadena susceptible de definición por parte del usuario.
problema	Problema de ITIL.
incident_priority	Prioridad de incidente de ITIL.
cambiar	call_req.change: entero que es el identificador exclusivo que hace referencia a una fila de la tabla chg. Indica la orden de cambios creada como resultado de la solicitud. call_req.change = chg.id.
service_type	srv_desc.sym: tipo de servicio real. call_req.support_lev = srv_desc.code
severity_num	sevrty.sym: número de severidad real. call_req.severity = sevrty.enum
urgency_num	urgncy.sym: número de urgencia real. call_req.urgency = urgncy.enum
category_name	prob_ctg.sym: área de solicitud real (categoría de problema). call_req.category = prob_ctg.id.
activo	ca_owned_resource.resource_name: nombre de activo real. call_req.affected_rc = ca_owned_resource.own_resource_uuid.
impact_num	impact.sym: número de impacto real. call_req.impact = impact.enum.
assignee_lastname	ca_contact.last_name: apellidos reales del asignatario. call_req.assignee = ca_contact.contact_uuid.
assignee_firstname	ca_contact.first_name: nombre real del asignatario. call_req.assignee = ca_contact.contact_uuid.

Campo	Observaciones
assignee_middlename	ca_contact.middle_name: segundo nombre real del asignatario. call_req.assignee = ca_contact.contact_uuid.
customer_lastname	ca_contact.last_name: apellidos reales del usuario final afectado. call_req.customer = ca_contact.contact_uuid.
customer_firstname	ca_contact.first_name: nombre real del usuario final afectado. call_req.customer.ca_contact.contact_uuid.
customer_middlename	ca_contact.middle_name: segundo nombre real del usuario final afectado. call_req.customer = ca_contact.contact_uuid.
group_name	View_Group.last_name: nombre real del grupo.
groupID	View_Group.contact_uuid: ID de clave real del grupo.
status_name	cr_stat.sym: estado real.
priority_num	pri.sym: número de prioridad real.

View_Request_to_Act_Log

Se trata de una vista básica de todas las solicitudes junto con sus registros de actividades. Se une la vista View_Request con la vista View_Act_Log para ofrecer información más detallada sobre cada una de las actividades por solicitud.

Campo	Observaciones
View_Request.*	Campos indicados en la definición anterior de la vista View_Request de este documento.
View_Act_Log.*	Campos indicados en la definición anterior de la vista View_Act_Log de este documento.

View_Request_to_Properties

Se trata de una vista básica de las solicitudes de llamada y sus propiedades. En ella se muestran todos los elementos de la tabla de solicitudes de llamada (call_req) y de la tabla de propiedades de solicitud (cr_prp).

Campo	Observaciones
View_Request.*	Campos indicados en la definición anterior de la vista View_Request de este documento.
crprp_id	cr_prp.id: entero que es el identificador exclusivo para el registro de la propiedad.
crprp_persid	cr_prp.persid: identificador exclusivo para el registro en la tabla cr_prp, precedido por el identificador de objeto (cr_prp) y dos puntos.
secuencia	cr_prp.sequence: entero que indica el orden en el que CA Service Desk Manager debe mostrar el registro de esta propiedad en particular (por, ejemplo, ascendente).
etiqueta	cr_prp.label: descripción breve del valor que se debe indicar en el campo cr_prp.value.
valor	cr_prp.value: valor introducido por el usuario en respuesta a los campos prp_description y cr_prp.label.
crprp_last_mod_dt	cr_prp.last_mod_dt: indicación de tiempo (pdmtime) que identifica cuándo se modificó por última vez la propiedad.
crprp_last_mod_by	cr_prp.last_mod_by: identificador binario que hace referencia a un registro de la tabla ca_contact. Representa la persona que ha modificado por última vez el registro. cr_prp.last_mod_by = ca_contact.contact_uid.
obligatorio	cr_prp.required: valor booleano que indica si la propiedad debe tener algún valor cr_prp.value para poder guardar el registro.
muestra	cr_prp.sample: campo de texto que muestra valores de ejemplo que sirven al usuario para introducir el valor más útil en el campo cr_prp.value.
owning_cr	cr_prp.owning_cr: identificador exclusivo empleado para identificar el registro específico al que se adjunta esta propiedad. cr_prp.object_id = call_req.persid.
crprp_description	cr_prp.description: campo de texto donde se explica el tipo de valor que se debe introducir en el campo cr_prp.value.

Apéndice B: RFC 2251: códigos de resultados de LDAP

Esta sección contiene los siguientes temas:

[Códigos devueltos de LDAP](#) (en la página 991)

[Códigos devueltos de servidores LDAP](#) (en la página 991)

[Códigos devueltos de clientes LDAP](#) (en la página 997)

[Estándares RFC asociados a LDAP](#) (en la página 999)

Códigos devueltos de LDAP

LDAP dispone de un conjunto de códigos de resultados de las operaciones que puede generar el servidor LDAP en respuesta a diversas solicitudes LDAP. Estos códigos indican el estado de la operación del protocolo y se clasifican por categorías de códigos devueltos de servidor o cliente.

Códigos devueltos de servidores LDAP

La siguiente tabla enumera los códigos devueltos de servidor:

Hexadecimal	Decimal	Descripción
0x00	0	LDAP_SUCCESS Indica que la operación del cliente solicitado ha finalizado de manera correcta.
0x01	1	LDAP_OPERATIONS_ERROR Indica que se ha producido un error interno. El servidor no es capaz de responder con algún error más específico ni tampoco de responder de manera adecuada a la solicitud. No significa que el cliente haya enviado un mensaje erróneo.
0x02	2	LDAP_PROTOCOL_ERROR Indica que el servidor ha recibido del cliente una solicitud que no es válida o tiene un formato incorrecto.
0x03	3	LDAP_TIMELIMIT_EXCEEDED Indica que se ha superado el límite de tiempo especificado por el cliente o el servidor para la operación. En las operaciones de búsqueda, se devuelven los resultados incompletos.

Hexadecimal	Decimal	Descripción
0x04	4	LDAP_SIZELIMIT_EXCEEDED En las operaciones de búsqueda, indica que se ha superado el límite de tamaño especificado por el cliente o el servidor. Se devuelven los resultados incompletos.
0x05	5	LDAP_COMPARE_FALSE No indica ninguna condición de error, sino que los resultados de las operaciones de comparación son falsos.
0x06	6	LDAP_COMPARE_TRUE No indica ninguna condición de error, sino que los resultados de las operaciones de comparación son verdaderos.
0x07	7	LDAP_AUTH_METHOD_NOT_SUPPORTED Indica que, durante la operación de enlace, el cliente ha solicitado un método de autenticación que no admite el servidor LDAP.
0x08	8	LDAP_STRONG_AUTH_REQUIRED Indica una de estas situaciones: ■ En las solicitudes de enlace, el servidor LDAP sólo acepta métodos de autenticación sólida. ■ En las solicitudes de los clientes, el cliente ha solicitado una operación (por ejemplo, una eliminación) que exige autenticación sólida. ■ En los avisos no solicitados de desconexión, el servidor LDAP detecta que la seguridad que protege las comunicaciones entre el cliente y el servidor ha fallado de forma inesperada o se ha visto comprometida.
0x09	9	Se trata de un código reservado.
0x0A	10	LDAP_REFERRAL No indica ninguna condición de error, pero, en LDAPv3, indica que el servidor no contiene la entrada de destino de la solicitud aunque quizá los servidores del campo de referencia sí lo hagan.
0x0B	11	LDAP_ADMINLIMIT_EXCEEDED Indica que se ha superado el límite del servidor LDAP definido por un usuario con autoridad administrativa.
0x0C	12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION Indica que el servidor LDAP no ha sido capaz de satisfacer la solicitud porque una o más de las extensiones críticas no se encontraban disponibles. Puede ser que el servidor no admita el control o que el control no sea adecuado para el tipo de operación.

Hexadecimal	Decimal	Descripción
0x0D	13	LDAP_CONFIDENTIALITY_REQUIRED Indica que la sesión no está protegida por ningún protocolo, como TLS (seguridad de la capa de transporte), que proporciona confidencialidad a las sesiones.
0x0E	14	LDAP_SASL_BIND_IN_PROGRESS No indica ninguna condición de error, sino que el servidor está listo para el paso siguiente del proceso. El cliente debe enviar al servidor el mismo mecanismo SASL para continuar el proceso.
0x0F	15	Este código no se usa.
0x10	16	LDAP_NO_SUCH_ATTRIBUTE Indica que el atributo especificado en la operación de modificación o de comparación no existe en la entrada.
0x11	17	LDAP_UNDEFINED_TYPE Indica que el atributo especificado en la operación de modificación o de adición no existe en el esquema del servidor LDAP.
0x12	18	LDAP_INAPPROPRIATE_MATCHING Indica que la regla de cotejo especificada en el filtro de búsqueda no coincide con ninguna regla definida para la sintaxis del atributo.
0x13	19	LDAP_CONSTRAINT_VIOLATION Indica que el valor del atributo especificado en la operación de modificación, de adición o de modificación de DN infringe las restricciones aplicadas al atributo. Éstas pueden ser de tamaño o de contenido (sólo cadenas, no valores binarios).
0x14	20	LDAP_TYPE_OR_VALUE_EXISTS Indica que el valor del atributo especificado en la operación de modificación o de adición ya existe como valor de dicho atributo.
0x15	21	LDAP_INVALID_SYNTAX Indica que el valor del atributo especificado en la operación de adición, de comparación o de modificación tiene una sintaxis que no es válida o reconocible para el atributo.
	22-31	Este código no se usa.
0x20	32	LDAP_NO_SUCH_OBJECT Indica que no se encuentra el objeto de destino. Este código no se devuelve en las siguientes operaciones: ■ Operaciones de búsqueda que encuentran la base de búsqueda pero no encuentran ninguna entrada que coincida con el filtro de búsqueda.

Hexadecimal	Decimal	Descripción
		■ Operaciones de enlace.
0x21	33	LDAP_ALIAS_PROBLEM Indica que se ha producido un error al anular la referencia de un alias.
0x22	34	LDAP_INVALID_DN_SYNTAX Indica que la sintaxis de DN es incorrecta. Ahora bien, si la sintaxis de DN es correcta pero las reglas de estructura del servidor LDAP no permiten la operación, el servidor devuelve lo siguiente: LDAP_UNWILLING_TO_PERFORM
0x23	35	LDAP_IS_LEAF Indica que no se puede realizar la operación especificada en una entrada de hoja. (Aunque este código no se encuentra actualmente en las especificaciones de LDAP, se reserva para esta constante.)
0x24	36	LDAP_ALIAS_DEREF_PROBLEM Indica que, durante la operación de búsqueda, el cliente carece de derechos de acceso para leer el nombre de los objetos con alias, o bien, no se permite la anulación de referencias.
	37-47	Este código no se usa.
0x30	48	LDAP_INAPPROPRIATE_AUTH Indica que, durante la operación de enlace, el cliente intenta usar un método de autenticación que no puede utilizar correctamente. Por ejemplo, cualquiera de las situaciones siguientes causa este error: ■ El cliente devuelve credenciales simples pero se exigen credenciales sólidas. ■ El cliente devuelve un DN y una contraseña para un enlace simple pero no se ha definido ninguna contraseña para la entrada.
0x31	49	LDAP_INVALID_CREDENTIALS Indica que, durante la operación de enlace, se ha producido una de estas situaciones: ■ El cliente ha transferido un DN o una contraseña incorrectos. ■ La contraseña es incorrecta porque ha vencido, la detección de un intruso ha bloqueado la cuenta o algún motivo parecido.
0x32	50	LDAP_INSUFFICIENT_ACCESS Indica que el autor de la llamada carece de derechos suficientes

Hexadecimal	Decimal	Descripción
		para realizar la operación solicitada.
0x33	51	LDAP_BUSY Indica que el servidor LDAP está demasiado ocupado para procesar la solicitud del cliente en ese momento pero que, si espera y vuelve a enviarla, es posible que el servidor pueda procesarla entonces.
0x34	52	LDAP_UNAVAILABLE Indica que el servidor LDAP no puede procesar la solicitud de enlace del cliente, por lo general, porque se está cerrando.
0x35	53	LDAP_UNWILLING_TO_PERFORM Indica que el servidor LDAP no puede procesar la solicitud debido a las restricciones definidas por el servidor. Este error se devuelve por los motivos siguientes: ■ La solicitud de adición de entrada infringe las reglas de estructura del servidor. ■ La solicitud de modificación de atributo especifica atributos que el usuario no puede modificar. ■ Las restricciones de contraseña impiden la ejecución de la acción. ■ Las restricciones de conexión impiden la ejecución de la acción.
0x36	54	LDAP_LOOP_DETECT Indica que el cliente ha detectado un alias o un bucle de referencias y, por lo tanto, no es capaz de finalizar la solicitud.
	55-63	Este código no se usa.
0x40	64	LDAP_NAMING_VIOLATION Indica que la operación de adición o de modificación de DN infringe las reglas de estructura del esquema. Por ejemplo: ■ La solicitud coloca la entrada en una posición subordinada a un alias. ■ La solicitud coloca la entrada en una posición subordinada a un contenedor que está prohibido según las reglas de contención. ■ El RDN de la entrada emplea un tipo de atributo prohibido.
0x41	65	LDAP_OBJECT_CLASS_VIOLATION Indica que la operación de adición, de modificación o de modificación de DN infringe las reglas de clases de objetos de la entrada. Por ejemplo, los tipos de solicitudes siguientes devuelven

Hexadecimal	Decimal	Descripción
		este error: ■ La operación de adición o de modificación intenta agregar una entrada que carece del valor de un atributo obligatorio. ■ La operación de adición o de modificación intenta agregar una entrada con un valor para un atributo que no existe en la definición de la clase. ■ La operación de modificación intenta eliminar un atributo obligatorio sin eliminar la clase auxiliar que define el atributo, si procede.
0x42	66	LDAP_NOT_ALLOWED_ON_NONLEAF Indica que la operación solicitada sólo se permite en las entradas de hoja. Por ejemplo, los tipos de solicitudes siguientes devuelven este error: ■ El cliente solicita una operación de eliminación en una entrada principal. ■ El cliente solicita una operación de modificación de DN en una entrada principal.
0x43	67	LDAP_NOT_ALLOWED_ON_RDN Indica que la operación de modificación ha intentado eliminar el valor de un atributo que forma el nombre completo relativo de la entrada.
0x44	68	LDAP_ALREADY_EXISTS Indica que la operación de adición ha intentado agregar una entrada que ya existe o que la operación de modificación ha intentado cambiar el nombre de una entrada al nombre de otra entrada que ya existe.
0x45	69	LDAP_NO_OBJECT_CLASS_MODS Indica que la operación de modificación ha intentado modificar las reglas de estructura de una clase de objeto.
0x46	70	LDAP_RESULTS_TOO_LARGE Este código está reservado para CLDAP.
0x47	71	LDAP_AFFECTS_MULTIPLE_DSAS Indica que la operación de modificación de DN mueve la entrada de un servidor LDAP a otro y que, por consiguiente, hace falta más de un servidor LDAP.
	72-79	Este código no se usa.
0x50	80	LDAP_OTHER

Hexadecimal	Decimal	Descripción
		Indica una condición de error desconocido. Se trata del valor predeterminado para los códigos de error NDS que no se corresponden con ningún otro código de error LDAP.

Códigos devueltos de clientes LDAP

La siguiente tabla enumera los códigos devueltos de cliente:

Hexadecimal	Decimal	Descripción
0x51	81	LDAP_SERVER_DOWN Indica que las bibliotecas LDAP no pueden establecer la conexión inicial con el servidor LDAP. Puede que el servidor LDAP no esté disponible o que el nombre de host o el número de puerto especificados sean incorrectos.
0x52	82	LDAP_LOCAL_ERROR Indica que se ha producido un error en el cliente LDAP. Por lo general, se trata de errores de asignación de memoria dinámica.
0x53	83	LDAP_ENCODING_ERROR Indica que el cliente LDAP ha encontrado errores al codificar la solicitud LDAP destinada al servidor LDAP.
0x54	84	LDAP_DECODING_ERROR Indica que el cliente LDAP ha encontrado errores al decodificar la respuesta LDAP del servidor LDAP.
0x55	85	LDAP_TIMEOUT Indica que se ha superado el límite de tiempo del cliente LDAP mientras se esperaba el resultado.
0x56	86	LDAP_AUTH_UNKNOWN Indica que se ha invocado la función <code>ldap_bind</code> o la función <code>ldap_bind_s</code> con un método de autenticación desconocido.
0x57	87	LDAP_FILTER_ERROR Indica que se ha invocado la función <code>ldap_search</code> con un filtro de búsqueda que no es válido.
0x58	88	LDAP_USER_CANCELLED Indica que el usuario ha cancelado la operación LDAP.
0x59	89	LDAP_PARAM_ERROR

Hexadecimal	Decimal	Descripción
		Indica que se ha invocado una función de LDAP con un valor de parámetro que no es válido (por ejemplo, el parámetro de ID es nulo).
0x5A	90	LDAP_NO_MEMORY Indica que se ha producido un error en la asignación de memoria dinámica al invocar la función de LDAP.
0B	91	LDAP_CONNECT_ERROR Indica que el cliente LDAP ha perdido la conexión o no puede establecerla con el servidor LDAP.
0x5C	92	LDAP_NOT_SUPPORTED Indica que el cliente no admite las funciones solicitadas. Por ejemplo, si el cliente LDAP se establece como cliente LDAPv2, las bibliotecas definen este código de error cuando el cliente solicita funciones de LDAPv3.
0x5D	93	LDAP_CONTROL_NOT_FOUND Indica que el cliente ha solicitado un control que no encuentran las bibliotecas en la lista de controles admitidos enviada por el servidor LDAP.
0x5E	94	LDAP_NO_RESULTS_RETURNED Indica que el servidor LDAP no ha enviado ningún resultado. Al invocar la función <code>ldap_parse_result</code> , no se incluye ningún código de resultado en la respuesta del servidor.
0x5F	95	LDAP_MORE_RESULTS_TO_RETURN Indica que existen más resultados encadenados al mensaje de resultados. Las bibliotecas definen este código cuando al invocar la función <code>ldap_parse_result</code> se revela la disponibilidad de más códigos de resultados.
0x60	96	LDAP_CLIENT_LOOP Indica que las bibliotecas LDAP han detectado un bucle. Por lo general, esto sucede cuando se siguen referencias.
0x61	97	LDAP_REFERRAL_LIMIT_EXCEEDED Indica que la referencia supera el límite de saltos, que determina a cuántos servidores puede acceder el cliente para recuperar datos. Por ejemplo, supongamos que se dan las siguientes condiciones: ■ El límite de saltos es dos. ■ La referencia apunta al servidor D, con el que sólo se puede establecer contacto por medio del servidor B (1 salto) que, a su vez, se pone en contacto con el servidor C (2 saltos) que,

Hexadecimal	Decimal	Descripción
		por fin, se pone en contacto con el servidor D (3 saltos). En estas condiciones, se supera el límite de saltos, por lo que las bibliotecas LDAP definen este código.

Estándares RFC asociados a LDAP

En la siguiente tabla se describen los estándares RFC asociados a LDAP disponibles.

RFC	Descripción
1274	COSINE y el esquema de Internet X.500
1275	Requisitos de replicación para proporcionar un directorio de Internet mediante X.500
1276	Extensiones de replicación y operaciones distribuidas para proporcionar un directorio de Internet mediante X.500
1308	Introducción ejecutiva a los servicios de directorio mediante el protocolo X.500
1309	Introducción técnica a los servicios de directorio mediante el protocolo X.500
1430	Plan estratégico para el desarrollo de un servicio de directorio de Internet X.500
1488	Representación de cadena de las sintaxis de atributo estándar de X.500
1558	Una representación de cadena de filtros de búsqueda LDAP
1617	Pautas de nomenclatura y estructuración para servicios piloto de directorio X.500
1777	Protocolo ligero de acceso a directorios (v. 2)
1778	Representación de cadena de las sintaxis de atributo estándar
1779	Representación de cadena de nombres completos
1804	Publicación de esquemas en directorios X.500
1823	Interfaz de programación de aplicaciones LDAP
1959	Un formato URL LDAP
1960	Una representación de cadena de filtros de búsqueda LDAP
2044	UTF -8: formato de conversión del estándar Unicode y de la norma ISO 10646
2164	Uso de directorios X.500/LDAP con fines de compatibilidad con la asignación de direcciones MIXER
2218	Esquema común para el servicio de páginas blancas de Internet
2247	Uso de dominios en nombres completos LDAP/X.500

RFC	Descripción
2251	Protocolo ligero de acceso a directorios (v. 3)
2252	Protocolo ligero de acceso a directorios (v3): definiciones de sintaxis de atributo
2253	Protocolo ligero de acceso a directorios (v3): representación de cadena de nombres completos con UTF-8
2254	Representación de cadena de filtros de búsqueda LDAP
2255	Formato URL LDAP
2256	Resumen del esquema de usuario de X.500(96) para su uso con LDAP v. 3
2279	UTF-8: formato de conversión de la norma ISO 10646
2293	Representación de tablas y subárboles en directorios X.500
2294	Representación de la jerarquía de direcciones de autor/destinatario en el árbol de información de directorio X.500
2307	Enfoque del uso de LDAP como servicio de información de la red
2377	Plan de nomenclatura para aplicaciones compatibles con directorios de Internet
2531	Esquema de características de contenido para sistemas de fax por Internet
2559	Protocolos operacionales de infraestructura de claves públicas de Internet X.509 (LDAP v. 2)
2587	Esquema de infraestructura de claves públicas de Internet X.509 (LDAP v. 2)
2589	Protocolo ligero de acceso a directorios (v3): extensiones para servicios de directorio dinámico
2596	Uso de los códigos de idioma en LDAP
2649	Control y esquema LDAP para el mantenimiento de firmas de operaciones
2657	RFC 2657: cliente LDAP v. 2 frente a Index Mesh
2696	Extensión de control LDAP para la manipulación de resultados con paginación simple
2713	Esquema de representación de objetos Java(tm) en directorios LDAP
2714	Esquema de representación de referencias de objetos CORBA en directorios LDAP
2739	Atributos de calendario para vCard y LDAP
2798	Definición de la clase de objeto LDAP inetOrgPerson
2820	Requisitos de control de acceso para LDAP
2829	Métodos de autenticación para LDAP
2830	Protocolo ligero de acceso a directorios (v3): extensión para la seguridad de la capa de transporte
2849	Formato de intercambio de datos LDAP (LDIF): especificaciones técnicas

RFC	Descripción
2879	Esquema de características de contenido para sistemas de fax por Internet (v. 2)
2891	Extensión de control LDAP para la ordenación desde el servidor de los resultados de búsqueda
3045	Almacenamiento de información de distribuidores en el DSE raíz de LDAP
3062	Operación extendida LDAP de modificación de contraseñas
3112	Esquema contraseñas de autenticación LDAP
3296	Referencias subordinadas nombradas en directorios LDAP
3377	Protocolo ligero de acceso a directorios (v. 3): especificaciones técnicas
3384	Protocolo ligero de acceso a directorios (v. 3): requisitos de replicación

Apéndice C: Comandos de referencia

Este apéndice proporciona comandos de referencia detallados disponibles para CA Service Desk Manager.

Esta sección contiene los siguientes temas:

[bop_sinfo](#): mostrar información del sistema (en la página 1004)
[dbmonitor_nxd](#): daemon de control de base de datos (en la página 1005)
[pdm_backup](#): escritura de bases de datos en archivos ASCII (en la página 1007)
[pdm_cache_refresh](#): actualización de bases de datos (en la página 1008)
[pdm_configure](#): apertura de la ventana de configuración (en la página 1010)
[pdm_d_refresh](#): inicio de demonios erróneos (en la página 1010)
[pdm_deref](#): anulación de referencias de datos ASCII (en la página 1011)
[pdm_discimp](#): importación de activos detectados (en la página 1015)
[pdm_discupd](#): actualización de activos detectados (en la página 1017)
[pdm_edit](#): configuración de procesos de servidor (en la página 1017)
[pdm_extract](#): extracción de datos de las bases de datos (en la página 1019)
[pdm_halt](#): finalización de demonios o detención de servicios (en la página 1023)
[pdm_init](#): inicio de demonios (en la página 1023)
[pdm_key_refresh](#): actualización de información de claves almacenada en caché (en la página 1024)
[pdm_lexutil](#): modificación de léxicos de CA Service Desk Manager (en la página 1024)
[pdm_k_reindex](#): utilidad de reindexación de conocimientos (en la página 1025)
[pdm_listconn](#): enumeración de conexiones activas (en la página 1031)
[pdm_load](#): adición, actualización y eliminación de registros de las bases de datos (en la página 1034)
[pdm_logfile](#): cambio del tamaño de corte de stdlog (en la página 1036)
[pdm_proctor_init](#): inicio del supervisor en servidores secundarios (en la página 1037)
[pdm_replace](#): reemplazo de tablas de bases de datos (en la página 1037)
[pdm_restore](#): restauración de bases de datos (en la página 1039)
[pdm_status](#): visualización del estado de demonios o procesos (en la página 1041)
[pdm_task](#): definición de variables de entorno (en la página 1041)
[pdm_text_cmd](#): interfaz de la línea de comandos de Text API (en la página 1042)
[pdm_uconv--](#): Conversión de un conjunto de caracteres local a UTF-8 (en la página 1045)
[pdm_userload](#): adición, actualización y eliminación de registros de las bases de datos (en la página 1048)
[pdm_webstat](#): devolución de estadísticas de uso Web (en la página 1051)
[report](#): generación de informes (en la página 1055)
[rpt_srv](#): generación de informes (en la página 1056)

[uniconv: inicio de daemon de conversor de eventos de CA NSM en UNIX](#) (en la página 1058)

bop_sinfo: mostrar información del sistema

La utilidad bop_sinfo muestra información sobre un solo objeto definido como Majic. Puede ejecutar esta utilidad en los objetos enumerados en la *Guía de referencia técnica*.

Sintaxis

Este comando tiene el formato siguiente:

```
bop_sinfo [-s servidor] [-p] [-l] [-d] [-f] [-q] [-t] [-m] [-a] objeto [-h]
```

-s servidor

Especifica el servidor en que se va a realizar la consulta.

-p

Muestra la información del productor.

-l

Muestra la lista de domset.

-d

Muestra la información de los objetos de la base de datos, incluidos el nombre y el tipo de todos los atributos.

-f

Muestra la información de tabla, incluidos rel_attr y common_name.

-q

Muestra el nombre de esquema de la tabla asociada.

-t

Muestra los desencadenadores del objeto.

-m

Muestra los métodos utilizados por el objeto.

-a

Muestra los detalles de atributos.

objeto

Nombre del objeto que se va a consultar

-h

Muestra la ayuda en la utilidad.

Ejemplo: mostrar información del sistema para el objeto dmn

```
bop_sinfo -d dmn
```

Factory dmn

Atributos

```
id                INTEGER
producer_id LOCAL STRING(20)
persistent_id     STRING(30)
sym              STRING(60) REQUIRED
delete_flag SREL -> actbool.enum REQUIRED
desc             STRING(40)
tables           BREL <- dcon.dom_id {dom_id = ?}
last_mod         DATE
last_mod_by SREL -> cnt.id
audit_useridLOCAL SREL -> cnt.id
```

dbmonitor_nxd: daemon de control de base de datos

El daemon de control de base de datos (dbmonitor_nxd) proporciona un mecanismo para permitir que se actualice la memoria caché de las tablas de base de datos específicas de CA Service Desk Manager cuando los cambios se realizan fuera de CA Service Desk Manager.

La función principal de dbmonitor_nxd es generar notificaciones de CAMBIOS para los cambios de las tablas especificadas que no se produjeron a través de CA Service Desk Manager. Para ejecutar esta función, el monitor consulta periódicamente la base de datos, determina lo que ha sido cambiado externamente y, a continuación, envía notificaciones de CAMBIOS al servidor de bpvirtodb_nxd. El servidor de bpvirtodb_nxd notifica del cambio a todos los servidores de domsrvr, lo que hace que cada servidor actualice la memoria caché de objetos específicos de la base de datos y, a continuación, notifique al resto de los procesos que suscriben los cambios en las tablas especificadas.

Este mecanismo funciona bien para los cambios externos eventuales en las tablas controladas. Sin embargo, en los casos en que las actualizaciones en masa se realizan externamente, se retransmite una tormenta de notificaciones de CAMBIOS que conduce a muchas consultas de base de datos desde distintos procesos de CA Service Desk Manager que repercuten significativamente en el rendimiento de CA Service Desk Manager.

Para eliminar este impacto sobre el rendimiento de CA Service Desk Manager, se ha actualizado dbmonitor_nxd en esta versión del producto. El monitor es compatible con una interfaz de línea de comandos que permite al usuario iniciar y detener el control de las tablas especificadas.

Sintaxis

Este comando tiene el formato siguiente:

```
dbmonitor_nxd -c <comando> -t <tablas>
```

<comando>

Escriba start o stop.

<tablas>

Especifica un nombre de tabla o una lista delimitada por comas de nombres de tabla que deben coincidir con una o más de las tablas especificadas en la variable de entorno NX_DBMONITOR_TABLES.

Cada solicitud se envía al daemon dbmonitor_nxd. El daemon lleva a cabo las acciones apropiadas y devuelve un mensaje al usuario que le indica la acción que se ha realizado.

- Si se invoca una solicitud de inicio en una tabla que ya se ha iniciado, no lleva a cabo ninguna acción.
- Si se invoca una solicitud de detención en una tabla que ya se ha detenido, no lleva a cabo ninguna acción.
- Si el control se detiene o se inicia correctamente en una tabla, también se escribe un mensaje de registro en stdlog.

Nota: Cuando se pausa el monitor de la tabla, es posible que todos los procesos de CA Service Desk Manager que almacenan los datos de estas tablas en la memoria caché se desactualicen, y la actualización de la memoria caché no está prevista.

Por ejemplo, BOPLGIN almacena en memoria caché los registros de contacto (provenientes de las tablas ca_contact y usp_contact) y esta memoria no se actualizará al realizar una pausa en el monitor para la tabla ca_contact durante el intervalo en que se cargaron actualizaciones externas en la base de datos. En el caso de BOPLGIN, este hecho tendrá poca repercusión porque los atributos básicos de los contactos almacenados en la memoria caché de BOPLGIN se toman de la tabla usp_contact y no de la tabla ca_contact.

Nota: Al realizar una pausa en el monitor de la tabla, los usuarios Web no podrán ver los cambios de la tabla cuando visualizan un formulario de detalles, si los cambios se realizaron externamente mientras el monitor estaba en pausa.

pdm_backup: escritura de bases de datos en archivos ASCII

pdm_backup detiene CA Service Desk Manager y, a continuación, escribe una o varias tablas de una base de datos de CA Service Desk Manager en un archivo ASCII. Puede utilizar este archivo de salida como el archivo de entrada para pdm_restore. Además del contenido de las bases de datos, pdm_backup realiza una copia de seguridad de los archivos de configuración de las aplicaciones.

Si se disponen de herramientas de copia de seguridad específicas del entorno operativo, es recomendable emplearlas en lugar de pdm_backup. Como pdm_backup es una herramienta genérica, su ejecución puede ser muy lenta en algunos entornos operativos.

Nota: como parte de su procesamiento, la utilidad pdm_backup cierra primero los daemon (UNIX) o los servicios (Windows).

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_backup [-d] [-g] [-v] -f filename [ALL | table1...tableN]
```

-d

Especifica la realización de una copia de seguridad de los datos de una base de datos solamente.

-g

Especifica que sólo se realiza la copia de seguridad de los datos que no sean de las bases de datos, es decir, que sólo se efectúa la copia de seguridad de las ventanas (formularios) y de otros datos ajenos a las bases de datos.

-v

Especifica el modo de detalles, que escribe comentarios acerca del progreso de los comandos en stdout.

-f nombre_de_archivo

Especifica un archivo de salida.

ALL|table1 ... tableN

Especifica TODOS los archivos o bien la tabla o las tablas que se deban escribir. Si se especifica más de una tabla, es preciso separarlas con espacios.

- Puede encontrar nombres de tabla en el archivo de esquema de la base de datos de CA Service Desk Manager, *ddict.sch*, que se encuentra en `$NX_ROOT/site` (UNIX) o *directorio-instalación\site* (Windows). `$NX_ROOT` o *directorio-instalación* es el directorio donde instaló CA Service Desk Manager.
- Si no se especifica ninguna tabla, se escribe la base de datos entera de CA Service Desk Manager, incluidos los grupos de ventanas y los archivos de registro de los menús.

Restricciones

no se puede ejecutar `pdm_backup` cuando CA Service Desk Manager esté activo.

Importante: En UNIX, `LIBPATH` debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice `pdm_task` para definir `LIBPATH` antes de ejecutar una utilidad. Por ejemplo, indique "`pdm_task pdm_clean_attachments ...`".

Más información:

[pdm_restore: restauración de bases de datos](#) (en la página 1039)

pdm_cache_refresh: actualización de bases de datos

`pdm_cache_refresh` provoca que los demonios o los procesos de CA Service Desk Manager usen los datos cargados en las bases de datos con `pdm_userload` u otras utilidades de las bases de datos, incluidas las herramientas de bases de datos ajenas a CA Service Desk Manager.

Casi todos los demonios y ejecutables de CA Service Desk Manager mantienen una caché en la memoria dinámica de los registros de las bases de datos. Esta memoria caché mejora el rendimiento ya que se elimina la necesidad de acceder a las bases de datos cuando los datos requeridos ya están disponibles. Los ejecutables de CA Service Desk Manager se notifican entre sí las actualizaciones de las bases de datos para que la caché se mantenga siempre al día. No obstante, no se produce esta notificación en el caso de las utilidades externas como, por ejemplo, `pdm_userload` u otras de terceros. Si se cargan datos nuevos en las bases de datos procedentes de uno de estos orígenes externos, es preciso ejecutar la utilidad `pdm_cache_refresh` para notificar a los módulos en ejecución que deben actualizar su caché con las bases de datos.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_cache_refresh [-f filename] [-t tablenamelist] [-d] [-v]
```

-f filename

Especifica un archivo de texto que contiene una lista de las tablas de bases de datos que se han modificado de forma externa. El archivo de texto consta de una o varias líneas, cada una de las cuales alberga el nombre de una tabla o los nombres de varias tablas separados por espacios.

-t tablename

Especifica una o más tablas que se han modificado de manera externa. Si la lista contiene más de una tabla, sus nombres deben ir separados por punto y coma, y la lista completa se debe encerrar entre comillas. Las tablas figuran en el apéndice "Diccionario de elementos de datos" de la *Guía de referencia técnica*.

Por ejemplo, supongamos que se han cargado datos sobre ubicaciones y departamentos en la base de datos de CA Service Desk Manager con una utilidad de terceros. Para indicar a los demonios de CA Service Desk Manager que actualicen su caché en lo relativo a dichas tablas, emita el siguiente comando:

```
pdm_cache_refresh -t "Ubicación;Sitio"
```

-d

Envía un mensaje a domsrvr, el servidor de dominios de CA Service Desk Manager. Acto seguido, éste vuelve a cargar todas las listas de selección, lo que provoca que parpadeen las ventanas de lista mostradas en los clientes.

-v

Especifica el modo de detalles. El valor 1 indica el modo breve. El valor 2 imprime los mensajes de progreso en el archivo de registro.

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

pdm_configure: apertura de la ventana de configuración

pdm_configure abre una ventana que contiene la ventana de configuración de CA Service Desk Manager. Utilice esta ventana para establecer la configuración de CA Service Desk Manager después de instalar CA Service Desk Manager o para cambiar la configuración de CA Service Desk Manager cuando CA Service Desk Manager esté en ejecución. Estas son algunas de las razones para cambiar la configuración de CA Service Desk Manager:

- Cambio del servidor o del tipo de base de datos
- Nueva carga de los datos predeterminados
- Cambie las contraseñas de las cuentas del sistema CA Service Desk Manager
- Regeneración de los archivos de esquema a fin de incorporar cambios
- Reconfiguración como servidor principal o como servidor secundario

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_configure
```

Restricciones

pdm_configure se puede ejecutar en un servidor de CA Service Desk Manager (principal o secundario) o un cliente Linux de CA Service Desk Manager. Es preciso ser el usuario con privilegios o el usuario raíz para ejecutar pdm_configure.

pdm_d_refresh: inicio de demonios erróneos

La utilidad de la línea de comandos pdm_d_refresh se emplea, sobre todo, para las configuraciones de daemons remotos. Insta al gestor de daemons a intentar iniciar los daemons en los que se ha producido algún error en el inicio después de diez intentos y que el propio gestor ha marcado como "no ejecutables". Ello sucede a menudo al iniciar el servidor principal cuando ocurre alguna de las siguientes posibilidades:

- No se ha iniciado todavía uno (o varios) de los servidores secundarios.
- Se ha detenido algún servidor secundario mientras el principal estaba en ejecución.

El gestor de daemons trata de iniciar los daemons remotos pero, si no se puede poner en contacto con el servidor secundario, lo intenta en diez ocasiones y finalmente se detiene. Al ejecutar esta utilidad, se marcan todos los daemons como ejecutables y se restablece el contador de reinicios. Después, el gestor de demonios intenta iniciar todos los demonios detenidos.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_d_refresh
```

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

pdm_deref: anulación de referencias de datos ASCII

pdm_deref procesa la entrada de datos con formato ASCII para intercambiar los datos que se encuentran en una tabla de una base de datos con los datos de otra tabla. Sirve para crear archivos compatibles con pdm_userload desde hojas de cálculo o bases de datos ajenas a CA Service Desk Manager. También se puede utilizar para crear informes o archivos de salida para hojas de cálculo o bases de datos ajenas a CA Service Desk Manager.

Importante: no utilice pdm_deref si no conoce a fondo el lenguaje SQL. Los directorios "export" e "import" de \$NX_ROOT/samples (UNIX) o directorio-instalación\samples (Windows) contienen un conjunto estándar de archivos de especificaciones para su consulta.

Sintaxis

Este comando tiene el formato siguiente:

```
name pdm_deref -s specfile [-c|-e|-r] [-d] [-h] [-n] [-u] [-v] <filename
```

-s specfile

(Obligatorio) Especifica un archivo que define los datos que se intercambian y las condiciones en las que se produce el cambio.

specfile contiene una lista de comandos SQL con el formato siguiente:

Deref

```
{
input = <lista de atributos "de" del archivo de entrada>
output = <lista de atributos "a" del archivo de salida>
rule = "SELECT <atributos empleados para rellenar los atributos de salida> \
      FROM <nombre de la tabla> \
      WHERE <atributo de la tabla que coincide con la entrada 1> =?\
      AND <atributo de la tabla que coincide con la entrada 2> = ? \
      O <atributo de la tabla que coincide con la entrada 3> =?"
}
```

-c

Produce una salida de valores separados por comas (CSV), por ejemplo:

"field1","field2","field3"

Las opciones de formato de la salida -c, -e y -r se excluyen mutuamente.

-e

Produce una salida de valores separados por comas (CSV) con comillas dobles incrustadas cuyo carácter de escape son otras comillas dobles. Por ejemplo:

"Texto con una "cadena entrecomillada"."

Las opciones de formato de la salida -c, -e y -r se excluyen mutuamente.

-r

Produce una salida con formato justificado a la izquierda si no se suministran las etiquetas de las columnas en el archivo de entrada:

"label":"value"

or

"value"

Esta opción se emplea con las impresoras en red, por ejemplo:

Field_Name: valor del campo

Las opciones de formato de la salida -c, -e y -r se excluyen mutuamente.

-d

Produce información de diagnóstico.

-h

Muestra información de ayuda y uso.

-n

Especifica que no se traten las claves externas cuyo valor sea 0 como nulas. Este argumento sólo se debe utilizar en circunstancias especiales al recuperar bases de datos dañadas.

-u

Produce una salida sin encabezados.

-v [1|2]

Especifica el modo de detalles. El valor 1 indica el modo breve. El valor 2 imprime los mensajes de progreso en el archivo de registro.

filename

(Opcional) Especifica el archivo de entrada con formato ASCII que se debe procesar. Si se omite, se emplea stdin.

Restricción: válido solamente en UNIX

Para utilizar pdm_deref en UNIX, es necesario definir antes la variable de entorno \$NX_ROOT en la ruta al directorio de instalación de CA Service Desk Manager y la variable de entorno PATH debe incluir \$NX_ROOT/bin.

Ejemplo: uso de pdm_deref para configurar los datos de la entrada

Este ejemplo muestra cómo utilizar pdm_deref para configurar los datos de la entrada.

Dados los siguientes datos en la tabla ca_location:

```
id      location_name_name
86873FA40BA4234A8CF7A418D7C8B2DB "Boulder NCC"
```

la siguiente instrucción del archivo de especificaciones:

```
Deref
{
input = place
output = location_uuid
rule = "SELECT id FROM ca_location WHERE location_name=?"
}
```

cambiaría la siguiente entrada:

```
last_name, first_name, place
{"Potts", "Elmore", "Boulder NCC"}
```

a la salida siguiente, que se puede cargar en la tabla ca.contact con pdm_userload:

```
last_name, first_name, location_uuid
{"Potts", "Elmore", "86873FA40BA4234A8CF7A418D7C8B2DB"}
```

Ejemplo: uso de pdm_deref para configurar los datos de la salida

Este ejemplo muestra cómo utilizar pdm_deref para configurar los datos de la salida.

Dados los datos siguientes en la tabla ca_contact:

```
id last_name first_name
"69499D5A2424884887E62EC9823F5E47" "Potts" "Elmore"
```

la siguiente instrucción del archivo de especificaciones:

```
Deref
{
input = primary_contact_uuid
output = firstname, lastname
rule = "SELECT first_name, last_name FROM ca_contact
WHERE id=?"
}
```

cambiaría la siguiente entrada:

```
location_name, primary_contact_uuid
{"Boulder NCC", "69499D5A2424884887E62EC9823F5E47"}
```

en la siguiente salida, que se puede imprimir en una hoja de cálculo o enviar a ésta:

```
location_name, firstname, lastname
{"Boulder NCC", "Elmore", "Potts"}
```

Más información:

[pdm_extract: extracción de datos de las bases de datos](#) (en la página 1019)

pdm_discimp: importación de activos detectados

Hace referencia al registro por lotes de los activos detectados ajenos a CA Service Desk Manager. Utilice esto para buscar activos en la base de datos de gestión que se muestran registrados por otros productos de software y registrarlos como activos de CA Service Desk Manager, de modo que pueda hacerse uso de ellos en CA Service Desk Manager.

La lógica es similar a la del cuadro de diálogo Activos detectados, que se abre desde los formularios Web de búsqueda y lista de activos. Es un proceso interactivo y por lotes.

Este programa realizará consultas en las tablas `ca_logical_asset`, `ca_asset` y `ca_logical_asset_property` con varios parámetros e intentará registrar activos de CA Service Desk Manager nuevos a partir de los valores detectados.

Sintaxis

```
pdm_discimp [-l label] [-s serial number] [-t asset tag] [-n hostname] [-d dns name] [-m mac address] [-c asset class] [-v] [-r] [-o object manager]
```

Criterios de selección de los activos (utilice el símbolo % como comodín):

o

Se buscan coincidencias con esta etiqueta.

s

Se buscan coincidencias con este número de serie.

t

Se buscan coincidencias con esta etiqueta de activo.

n

Se buscan coincidencias con este nombre de host.

Criterios de selección de las propiedades de activo (utilice el símbolo % como comodín):

d

Se buscan coincidencias con este nombre de DNS.

he

Se buscan coincidencias con esta dirección MAC.

Otras opciones:

c

Indica la clase de activo que se asigna al registrar los nuevos activos de propiedad; el valor predeterminado es Hardware detectado.

t

Especifica el modo de detalles o de diagnóstico.

r

Indica que se registren los activos; de lo contrario, se ejecuta en modo de simulación.

h

Muestra esta información.

o

Hace referencia al gestor de objetos (domsrvr) que se utiliza para el procesamiento.

Nota: Si el procesamiento da como resultado una etiqueta de activo en blanco, se usa como tal el valor encontrado para el nombre del host o el nombre de DNS. Los activos deben contar al menos con una etiqueta y clase de activo para poder utilizarse en CA Service Desk Manager.

Debido a las limitaciones en la estructura de la arquitectura de CA Service Desk Manager y la base de datos de gestión, se llevan a cabo dos consultas con el objetivo de seleccionar los registros adecuados para el procesamiento. Es importante tener esto claro, ya que puede afectar al rendimiento. La primera consulta recupera las filas de la unión de las tablas `ca_logical_asset` y `ca_asset` que tienen los mismos valores en la etiqueta de rotulación, el número de serie, la etiqueta y el nombre de host. Seguidamente, por cada fila resultante tiene lugar una consulta en la tabla `ca_logical_asset_property` para buscar coincidencias entre `dns_name` y `mac_address`. El activo de la primera consulta se selecciona para el registro si la segunda consulta devuelve alguna fila como resultado.

Importante: En UNIX, `LIBPATH` debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice `pdm_task` para definir `LIBPATH` antes de ejecutar una utilidad. Por ejemplo, indique "`pdm_task pdm_clean_attachments ...`".

pdm_discupd: actualización de activos detectados

Actualización por lotes de los activos detectados ajenos a CA Service Desk Manager. Utilice esta utilidad para actualizar los activos que han sido importados por el comando `pdm_discimp`.

Sintaxis

```
pdm_discupd [-t] [-v] [-d domsrvr]
```

Donde

t

Prueba

t

Especifica el modo de detalles o de diagnóstico.

d

Hace referencia al gestor de objetos (domsrvr) que se utiliza para el procesamiento.

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

pdm_edit: configuración de procesos de servidor

`pdm_edit` se emplea para editar el archivo de plantillas de inicio, `pdm_startup.tpl`, en el servidor de CA Service Desk Manager. La modificación del archivo de inicio de plantillas es necesaria, por ejemplo, para definir alias de los motores de objetos, para configurar la ejecución de los motores Web en servidores secundarios o para establecer la autenticación remota en servidores secundarios.

En UNIX:

Los usuarios de UNIX deben cambiar los permisos en el archivo `pdm_edit.pl` para hacerlo "ejecutable".

Sintaxis

En la instalación del servidor de CA Service Desk Manager, cambie al directorio \$NX_ROOT/samples/pdmconf (UNIX) o al *directorio-instalación*\samples\pdmconf (Windows) y, a continuación, escriba el siguiente comando para iniciar pdm_edit:

```
pdm_perl pdm_edit.pl
```

Nota: pdm_edit es un script en Perl, por lo que es aconsejable utilizar la versión de Perl que acompaña a CA Service Desk Manager, pdm_perl, para ejecutarla; no obstante, es posible que también funcionen otras versiones de Perl.

Uso

Una vez que pdm_edit está en ejecución, se solicita cierta información y el resto del proceso se desarrolla por medio de menús. Para obtener información sobre el uso, sírvase de la opción de menú H, con la que se ofrece ayuda. También puede acceder a la ayuda en el archivo pdm_edit.README, que se consulta con cualquier editor de texto.

Salida

Al salir de pdm_edit y guardar los cambios, se crean varios archivos:

- pdm_startup.rmt, que almacena los nuevos valores de configuración.
- alias_install.sh (UNIX) o alias_install.bat (Windows), si se han definido alias del motor de objetos.
- pdm_startup.dat, que almacena los datos necesarios para la próxima vez que se invoque pdm_edit (guarde este archivo en el directorio de trabajo con pdm_edit.pl).

Para aplicar los cambios efectuados, siga estos pasos:

1. Cree una copia de seguridad del archivo pdm_startup.tpl que reside en el directorio \$NX_ROOT/pdmconf (UNIX) o *directorio-instalación*\pdmconf (Windows) de la instalación del servidor principal de CA Service Desk Manager y, a continuación, use el archivo pdm_startup.rmt recién creado para reemplazarlo.

Nota: El usuario con privilegios debe poder leer el archivo pdm_startup.tpl creado a partir del archivo pdm_startup.rmt.

2. Si se han definido alias del motor de objetos, ejecute la secuencia de comandos alias_install para volver a configurar el servidor principal.

3. Ejecute la utilidad de configuración en el servidor principal de CA Service Desk Manager sin hacer ningún cambio. La configuración nueva surtirá efecto la próxima vez que inicie el servidor de CA Service Desk Manager.
4. Si es necesario, inicie todos los servidores secundarios de CA Service Desk Manager y, a continuación, inicie el servidor principal.

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

Más información:

[Inicio del servidor principal](#) (en la página 38)

[Inicio de servidores secundarios](#) (en la página 37)

pdm_extract: extracción de datos de las bases de datos

El comando *pdm_extract* permite extraer datos de las tablas especificadas de las bases de datos de CA Service Desk Manager o de la base de datos de CA Service Desk Manager completa. La salida consiste en texto con formato ASCII.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_extract [-c|-e|-r] [-d] [-h] [-u] [-v] [-C] [--B] [-f formatstring] ALL |
table1. . . TableN]
```

-c

Produce una salida de valores separados por comas (CSV), por ejemplo:

```
"field1","field2","field3"
```

Las opciones de formato de la salida -c, -e y -r se excluyen mutuamente.

-e

Produce una salida de valores separados por comas (CSV) con comillas dobles incrustadas cuyo carácter de escape son otras comillas dobles. Por ejemplo:

```
"Texto con una "cadena entrecomillada"."
```

Las opciones de formato de la salida -c, -e y -r se excluyen mutuamente.

-r

Produce una salida con formato justificado a la izquierda si no se suministran las etiquetas de las columnas en el archivo de entrada:

```
"label": "value"
```

or

```
"value"
```

Esta opción se emplea con las impresoras en red, por ejemplo:

Field_Name: valor del campo

Las opciones de formato de la salida -c, -e y -r se excluyen mutuamente.

-d

Emplea el formato de fecha que aparezca en el archivo \$NX_ROOT/fig/english/cfg/dataent.fmt (UNIX) o *directorio-instalación*\fig\english\cfg\dataent.fmt (Windows), el cual se puede editar conforme a las necesidades.

-h

Muestra información de ayuda y uso.

-u

Produce una salida sin encabezados.

-v

Especifica el modo de detalles, que escribe comentarios acerca del progreso de los comandos en stdout.

-C

Cambios que codifican de UTF-8 a otro conjunto de caracteres. El resultado predeterminado es UTF-8.

Ejemplo: Para convertir el resultado a JIS, puede ejecutar "-C iso-2022-jp"

Ejemplo: Para codificar al conjunto de caracteres nativo del sistema operativo, utilice "PREDETERMINADO" o "NATIVO".

-B

Suprime la marca de orden de bytes si la variable NX_ADD_UTF8_BYTE_ORDER_MARK está establecida.

La opción NX_ADD_UTF8_BYTE_ORDER_MARK es una firma en un archivo. Permite a los editores que admiten UTF-8 mantener la integridad de UTF-8 del archivo.

Nota: Sólo es necesario para datos que no son ASCII. Si no está instalado, el comportamiento predeterminado omite la marca de orden de bytes (BOM). Si está instalado, establézcalo en "1" o "Sí".

-f *formatstring*

Extrae determinados registros y campos de acuerdo con *formatstring*, que es una instrucción de un subconjunto SQL.

En el caso de fechas tras un período, utilice la siguiente sintaxis:

```
pdm_extract -v -f "select id, ref_num from Call_Req where open_date >=
DATE '2005-02-24'" > daterange1.txt
```

En el caso de intervalos de fechas, utilice la siguiente sintaxis:

```
pdm_extract -v -f "select id, ref_num from Call_Req where open_date >=
DATE '2004-01-20' and open_date < DATE '2004-02-25'" >
daterange2.txt
```

Nota: Incluya las fechas que estén en el formato YYYY-MM-DD entre comillas simples.

La sintaxis para DATE es:

```
DATE 'yyyy-mm-dd'
```

yyyy = entero que representa el año (entre 1970 y 2038)

mm = entero que representa el mes

dd = entero que representa el día

Ejemplos:

```
DATE '2005-01-18'
```

```
DATE '1999-12-25'
```

Ésta es la sintaxis de TIMESTAMP:

TIMESTAMP 'yyyy-mm-dd hh.mm.ss[.nnnnnn][[+|-][hh.mm]]

yyyy = entero que representa el año (entre 1970 y 2038)

mm = entero que representa el mes

dd = entero que representa el día

hh = entero que representa la hora

mm = entero que representa los minutos

ss = entero que representa los segundos

nnnn = entero opcional que representa las fracciones de segundo

[+|-][hh.mm] = intervalo de huso horario opcional

Ejemplos:

TIMESTAMP '1998-04-28 12:00:00.000000'

TIMESTAMP '2004-10-17 18:30:45'

TIMESTAMP '2005-03-21 12:00:12+08:00'

TIMESTAMP '1999-05-10 09:12:23.005-03:30'

Nota: La opción -d no es necesaria ya que únicamente afecta al formato de la salida.

Ejemplo de uso del comando:

```
pdm_extract -f "select * from Call_Req where open_date > TIMESTAMP '2004-01-12 12:00:00'"
```

En este ejemplo, todas las columnas se extraen de la tabla Call_Req y open_date es la medianoche del día doce de enero de 2004.

TODO

Extrae la salida de todas las tablas de la base de datos.

tabla1. . . TablaN

Extrae la salida de las tablas especificadas. Los nombres de las tablas se deben separar con espacios.

El formato predeterminado, si no se especifica ninguno, consiste en un archivo ASCII compatible con pdm_userload.

Más información:

[pdm_deref: anulación de referencias de datos ASCII](#) (en la página 1011)

[pdm_replace: reemplazo de tablas de bases de datos](#) (en la página 1037)

[pdm_userload: adición, actualización y eliminación de registros de las bases de datos](#) (en la página 1048)

[rpt_srv: generación de informes](#) (en la página 1056)

pdm_halt: finalización de demonios o detención de servicios

pdm_halt finaliza de forma segura todos los demonios de (UNIX) o servicios del servidor (Windows) de CA Service Desk Manager del sistema en el que se ejecute. La utilidad pdm_halt suele tardar unos 30 segundos en terminar. Si no avanza durante más de dos minutos, pulse las teclas Ctrl+C para detener pdm_halt y, a continuación, escriba **pdm_halt -F**.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_halt [-F]
```

-F

Se salta los procedimientos normales de cierre de daemon o servicios y los finaliza. CA Service Desk Manager le solicita confirmación. Si se impone la finalización de los demonios o los servicios, es posible que no se registren algunos de los procesos de las aplicaciones que estén en curso.

Restricciones

pdm_halt se puede ejecutar en un servidor de CA Service Desk Manager o un cliente UNIX de CA Service Desk Manager. Es preciso ser el usuario con privilegios para ejecutar pdm_halt.

pdm_init: inicio de demonios

Aplicable sólo a UNIX

pdm_init inicia todos los procesos automáticos de CA Service Desk Manager en el sistema en el que se ejecute. Estos procesos automáticos se denominan *daemon* y se ejecutan de forma continua en segundo plano mientras se trabaja. No todos los demonios se inician; algunos sólo son aplicables a determinados sistemas operativos. Consulte el capítulo "Gestión de servidores" para conocer la lista de daemon que este comando puede iniciar.

Nota: Utilice pdm_d_refresh para iniciar los daemon que no se hayan podido iniciar la primera vez después de haber solucionado el problema que haya impedido su inicio. En la mayoría de los casos, no hace falta finalizar los demonios en ejecución para iniciar los demonios cuyo inicio haya fallado.

Sintaxis

```
pdm_init
```

Restricciones

pdm_init se puede ejecutar en un servidor de CA Service Desk Manager o un cliente UNIX de CA Service Desk Manager. Es preciso ser el usuario con privilegios para ejecutar pdm_init.

pdm_key_refresh: actualización de información de claves almacenada en caché

La utilidad pdm_key_refresh actualiza la información de claves almacenada en caché con la tabla de control de claves de la base de datos. Cuando se actualice la información de control de las claves, basta con ejecutar esta utilidad; no hace falta detener y reiniciar el sistema para obligar a CA Service Desk Manager a utilizar los nuevos valores base de los ID de clave.

Importante: al cambiar la tabla de control de claves, se pueden provocar daños en los datos. No intente cambiar el control de claves sin instrucciones específicas del Soporte técnico de CA.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_key_refresh
```

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

pdm_lexutil: modificación de léxicos de CA Service Desk Manager

La utilidad pdm_lexutil permite modificar léxicos de Service Desk, para agregar o eliminar palabras del diccionario de revisión ortográfica.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_lexutil -a | -d [-f] [-l] lista de palabras
```


-a

Agrega palabras.

-d

Elimina palabras.

-f

Archivo o léxico que contiene la lista de palabras para agregar o eliminar.

-l

Nombre del léxico.

Valor predeterminado: userdict.tlx

lista de palabras

Palabras para agregar o eliminar.

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

pdm_k_reindex: utilidad de reindexación de conocimientos

La utilidad de reindexación de conocimientos, *pdm_k_reindex.exe*, se ubica en el directorio de instalación de Gestión del conocimiento. También puede utilizar esta utilidad en una integración de FAST ESP (see page 1028).

Nota: La reindexación de los documentos de la base de conocimiento puede requerir mucho tiempo, dependiendo del tamaño de la base de datos. Por lo tanto, es aconsejable ejecutar la utilidad de reindexación de conocimientos después de haber realizado todos los cambios que procedan.

Para ejecutar esta utilidad, escriba el siguiente comando en el símbolo del sistema:

```
pdm_k_reindex
```

A continuación, se indican las opciones disponibles con este comando.

Interfaz:

-D

Define el modo de depuración, por ejemplo, la impresión en la ventana de comandos.

-v

Define el modo de detalles, por ejemplo, la impresión en el archivo stdlog.

-i

No se crean índices de tabla en la tabla reindexada después de la reindexación.

Nota: Los parámetros que comiencen por guión (como "-D") deben ir delante de los demás parámetros.

archivo:reindex.txt

Los documentos se reindexan en el archivo adecuado.

+i

Sólo se crean índices de la tabla reindexada, que se convierte en la tabla de búsqueda después de la reindexación. Los índices antiguos se omiten antes de la reindexación.

+t

Sólo se cambian los nombres de las tablas de búsqueda y reindexación.

Nota: Un prefijo "+" indica que sólo se aplica este parámetro.

sdtout

Define la frecuencia de las estadísticas que aparecen en la ventana de comandos. De forma predeterminada, la utilidad de reindexación de conocimientos proporciona estadísticas en la ventana de comandos por cada 1.000 documentos procesados. No obstante, en ocasiones se necesitan estadísticas con mayor frecuencia. Emplee el siguiente parámetro:

```
pdm_k_reindex -i sdtout:10
```

En este ejemplo, se muestran estadísticas en la ventana de comandos por cada 10 documentos.

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

Cuándo utilizar pdm_k_reindex

Ejecute la utilidad pdm_k_reindex si se modifica al menos uno de los siguientes valores de búsqueda:

- Palabras irrelevantes
- Sinónimos
- Términos especiales

- Idioma
- Eliminar palabras similares
- Eliminar palabras irrelevantes
- Rango de caracteres válido
- Reconocer términos especiales

Cada vez que se produce algún cambio, aparece el mensaje correspondiente en el nodo Conocimientos de la ficha Administración.

Puede utilizar pdm_k_reindex con o sin una integración de FAST ESP:

- Utilice pdm_k_reindex sin FAST ESP (see page 1025)
- Utilice pdm_k_reindex con FAST ESP (see page 1028)

Seguimiento de reindexación

Mientras se ejecuta la reindexación, se puede ver el estado del proceso en la sección Seguimiento de reindexación de la mitad inferior de la página. Éstos son los campos:

Documento núm.

Especifica el número de documentos que ya se han procesado.

Tamaño medio (palabras)

Especifica el tamaño de los documentos actuales, que se calcula restando al número de palabras el número de palabras irrelevantes.

Velocidad (documentos/seg.)

Especifica el número de documentos procesados por segundo.

Tiempo desde el inicio

Indica la duración del proceso de reindexación desde su inicio.

Tiempo restante

Especifica el tiempo restante estimado del proceso, que se basa en la velocidad actual y el número restante de documentos.

Número de fallos

Representa el número de documentos fallidos (máximo = 100). Si se alcanza el número máximo de fallos, se pregunta al administrador si se debe continuar con el proceso o se debe cancelar.

Nota: Si se han realizado cambios en palabras irrelevantes, términos especiales, sinónimos o valores de análisis y no reindiza, se le pregunta la siguiente vez que acceda al nodo Conocimientos de la ficha Administración. Los cambios se aplicarán sólo después de ejecutar la utilidad de reindexación de conocimientos.

Importación y reindexación

Al invocar pdm_kit.exe en la línea de comandos, la utilidad pdm_kit importa los documentos a la base de datos oportuna. Una vez terminada la ejecución de pdm_kit, siempre que no se hayan desactivado la indexación o la reindexación de los documentos mediante las opciones de la línea de comandos, se invoca de forma automática la utilidad de reindexación (pdm_k_reindex.exe). El estado y la salida de la operación de reindexación se escriben automáticamente en el archivo "EBR_REINDEX.LOG" del directorio \$NX_ROOT\log.

Nota: Cuando se integra con FAST ESP, no se invoca la utilidad pdm_k_reindex porque los documentos se indexan en segundo plano.

Utilice pdm_k_reindex con FAST ESP

La utilidad pdm_k_reindex se utiliza para reindexar, desindexar y sincronizar selectivamente (reindexar y desindexar) tablas de documentos como KD, cr, iss, etc. La utilidad se invoca de la siguiente manera:

```
pdm_k_reindex [operación] [tabla] [modo]
```

operación

Las siguientes operaciones son válidas:

-h

Muestra la ayuda en la utilidad.

index

(Predeterminado) reindexa los documentos.

deindex

Desindexa los documentos.

sync

Permite reindexar y/o desindexar documentos para sincronizar el motor de búsqueda después de ejecutar el borrado definitivo o la restauración. En la operación sync son válidos los siguientes modos:

- **depurar**
sincronizar el motor de búsqueda después de ejecutar el borrado definitivo.
- **restore**
sincronizar el motor de búsqueda después de ejecutar la restauración.

estado

Muestra un recuento de los documentos que quedan por procesar.

tabla

Las siguientes tablas son válidas:

all

Define todas las tablas.

KD

(Predeterminado) Define la tabla KD.

cr

Define la tabla cr.

iss

Define la tabla iss.

mode

Los siguientes modos son válidos:

depurar

Sincroniza el motor de búsqueda después de la ejecución del borrado definitivo.

restore

Sincroniza el motor de búsqueda después de la ejecución de la restauración.

Nota: Si no se seleccionan argumentos de operación o de tabla, se indexa la tabla KD.

Parámetros de index de ejemplo

```
pdm_k_reindex [index] [factory:KD|cr|iss|all]
```

Parámetros de deindex de ejemplo

```
pdm_k_reindex deindex factory:KD|cr|iss|all [clearrange]
```

clearrange

(Opcional) Desindexa documentos que están fuera del intervalo predefinido de la tabla.

Nota: Con el parámetro deindex se debe especificar un argumento de tabla .

Parámetros de sync de ejemplo

```
pdm_k_reindex sync[:purge|restore] factory:KD|cr|iss|all
```

Nota: Si omite los modos purge o restore, se invocarán ambos modos. Con el parámetro sync también se debe especificar un argumento de tabla .

Parámetros varios

```
pdm_k_reindex -pm
```

Corrige las imágenes incrustadas y los vínculos del documento dentro del campo de resolución.

```
pdm_k_reindex -ml
```

Corrige los vínculos del documento dentro del campo de resolución y los asigna a la base de datos.

Nota: Para obtener más información sobre la utilidad pdm_k_reindex, consulte la *Guía de implementación*.

Reindexación y desindexación de la configuración de colas para procesamiento instantáneo y por lotes

Tanto la reindexación como la desindexación ejecutan un proceso por lotes, para incluir en una ejecución una cantidad de documentos predefinida. Estos procesos por lotes se utilizan para optimizar el rendimiento. El rendimiento del sistema aumenta cuanto más documentos se incluyan en el lote.

El número de documentos que se puede procesar es limitado; el límite depende del tamaño de los documentos y de los archivos adjuntos vinculados. El tamaño del documento se calcula en función del texto puro y sus adjuntos. No se consideran los elementos de imagen y formato.

Nota: Puede limitar el tamaño de los adjuntos; para ello, vaya a Biblioteca de adjuntos, Repositorios en la ficha Administración y edite el repositorio para establecer el tamaño límite del archivo (KB).

El tamaño máximo de lote recomendado se encuentra entre 2 y 12 MB (de acuerdo con el parámetro EBR_MAX_INDEX_BATCH_SIZE del archivo NX.env y el tamaño medio del documento).

- Si el tamaño medio del documento (incluidos los adjuntos) es de 0,1 MB aproximadamente, conserve la definición predeterminada en NX.env:

```
@EBR_MAX_INDEX_BATCH_SIZE=128
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=1
@NX_EBR_INDEX_QUEUE_ONLINE=Yes
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
```

Esta definición significa que un lote procesa 128 documentos, que las ejecuciones de los lotes se realizan cada intervalos de diez segundos y que cuando se ejecuta una reindexación, el intervalo de espera entre dos lotes es de un segundo.

- Si el tamaño medio del documento (incluidos los adjuntos) es de 0,5 MB aproximadamente, conserve la definición predeterminada en NX.env:

```
@EBR_MAX_INDEX_BATCH_SIZE=25
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=10
@NX_EBR_INDEX_QUEUE_ONLINE=No
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
```

Esta definición significa que un lote procesa 25 documentos, que las ejecuciones de los lotes se realizan cada intervalos de diez segundos y que cuando se ejecuta una reindexación, el intervalo de espera entre dos lotes es de diez segundos.

pdm_listconn: enumeración de conexiones activas

La utilidad pdm_listconn sirve para enumerar las conexiones activas tanto de los clientes como de los servidores.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_listconn [-c] [-s] [-s -c] [-t nn] [proc1 [proc2...]]
```

Si no se especifican parámetros, el comando predeterminado tiene el siguiente formato:

```
pdm_listconn -s -t 2
```

-c

Se muestran las conexiones por cliente. La utilidad muestra dos líneas por cada cliente:

```
(n secs) tipo_cliente nodo|proceso_cliente  
connected to alias (proceso_servidor) at momento
```

n es el número de segundos que ha tardado en responder el cliente.

tipo_cliente es "vbop", "animator daemon" o "web engine".

nodo es la dirección IP del nodo del cliente.

proceso_cliente es el nombre del proceso slump del cliente.

alias es el alias del servidor al que está conectado el cliente.

proceso_servidor es el nombre del proceso slump del servidor.

momento es el momento de conexión.

Por ejemplo:

```
(0 secs) vbop client 141.202.211.34|vbop-0x40120000:anthill:0  
connected to CMD40120 on anthill (domsrvr) at 02/19/1999 10:44:16
```

-s

Se muestran las conexiones por servidor (valor predeterminado). La utilidad muestra dos líneas por cada servidor:

```
(n secs) server alias (nodo|proceso_servidor) willingness disposición  
recuento connected clients (use pdm_listconn -c -s to list clients by server)
```

n es el número de segundos que ha tardado en responder el servidor.

nodo es la dirección IP del nodo del servidor.

alias es el alias del servidor al que está conectado el cliente.

proceso_servidor es el nombre del proceso slump del servidor.

disposición es la inclinación del servidor a aceptar clientes nuevos (de 0 a 100).

recuento es el número de clientes conectados.

Por ejemplo:

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients (use pdm_listconn -c -s to list clients by server)
  vbop client 141.202.211.34|vbop2 connected 02/19/1999 10:53:16
  vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 02/19/1999
10:44:17
```

-s -c

Se muestran las conexiones por servidor, incluidos los detalles sobre los clientes de cada servidor. La utilidad muestra varias líneas por cada servidor:

```
(n secs) server alias (nodo|proceso_servidor) willingness disposición
recuento connected clients:
tipo_cliente nodo|proceso_cliente connected momento
```

donde:

n es el número de segundos que ha tardado en responder el servidor.

nodo es la dirección IP del nodo del servidor.

alias es el alias del servidor al que está conectado el cliente.

proceso_servidor es el nombre del proceso slump del servidor.

disposición es la inclinación del servidor a aceptar clientes nuevos (de 0 a 100).

recuento es el número de clientes conectados.

tipo_cliente es "vbop", "animator daemon" o "web engine".

nodo es la dirección IP del nodo del cliente.

proceso_cliente es el nombre del proceso slump del cliente.

momento es el momento de conexión.

Por ejemplo:

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients:
  vbop client 141.202.211.34|vbop2 connected 02/19/1999 10:53:16
  vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 02/19/1999
10:44:17
```

-t nn

Especifica un intervalo de tiempo de espera en segundos. Como pdm_listconn recibe datos de un número desconocido de clientes y servidores, finaliza cuando transcurre el intervalo de tiempo de espera especificado después de la recepción del último mensaje.

Valor predeterminado: 2

proc1

Indica uno o más nombres de procesos slump separados por espacios. La utilidad muestra información del cliente o del servidor, según proceda.

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

pdm_load: adición, actualización y eliminación de registros de las bases de datos

Importante: el uso de pdm_load puede ser peligroso, por lo que antes de ejecutarlo, realice siempre una copia de seguridad de la base de datos y utilice pdm_userload en su lugar, a menos que se le inste a ejecutar pdm_load.

pdm_load actualiza la base de datos de CA Service Desk Manager con el archivo de entrada que se especifique hasta un máximo de 112 atributos.

Cada vez que se carguen partes (como solicitudes o incidencias), el número de parte debe incluir un prefijo o un sufijo exclusivo en la cadena. CA Service Desk Manager considera este número como una cadena de caracteres, no como un número secuencial y, por ello, no puede garantizar la asignación de un número exclusivo a los tickets cargados. Mientras se asigne un prefijo o un sufijo exclusivo con awk u otro procesador de textos, es posible cargar partes sin que CA Service Desk Manager escriba encima de los números asignados con anterioridad.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_load [-c] [-h] [-m] [-r] [-u] [-v] -f filename
```

Las entradas del archivo de entrada siguen este formato:

```
TABLE nombre_tabla
nombrecampo1 nombrecampo2. . . nombrecampoN
{ "valor11", "valor12", . . . "valor1N"}
{"valor21", "valor22", . . . "valor2N"}
.
.
.
{"valorN1", "valorN2", . . . "valorNN"}
```

table_name es el nombre de la tabla que se va a cargar, tal y como aparece indicado en el archivo de esquema de base de datos de CA Service Desk Manager, que está ubicado en \$NX_ROOT/site/schema.sch (UNIX) o *directorio-instalación*\site\schema.sch (Windows). \$NX_ROOT o *directorio-instalación* es el directorio donde instaló CA Service Desk Manager.

-f *nombre_de_archivo*

Especifica un archivo ASCII de entrada.

-c

Coteja el archivo de entrada con la base de datos y se limita a informar sobre las actualizaciones que habría que realizar (no las lleva a cabo).

-m

Especifica una actualización en masa. Se especifica cuando se emplea pdm_load para agregar o eliminar un número elevado de registros. Esta opción suprime todas las notificaciones de actualización de los clientes y envía un mensaje de actualización de la caché de la tabla pertinente cuando pdm_load termina de procesarla.

-r

Elimina los registros de la base de datos que coincidan con los registros de entrada.

Importante: realice una copia de seguridad de la base de datos antes de ejecutar pdm_load con esta opción. Después de eliminar los registros antiguos de la base de datos, es preciso restaurar la base de datos de CA Service Desk Manager con esta copia de seguridad si se desea recuperar alguno de ellos.

-u

Actualiza los registros existentes pero no inserta ningún registro nuevo en la base de datos.

Más información:

[pdm_backup: escritura de bases de datos en archivos ASCII](#) (en la página 1007)

[pdm_replace: reemplazo de tablas de bases de datos](#) (en la página 1037)

[pdm_restore: restauración de bases de datos](#) (en la página 1039)

[pdm_userload: adición, actualización y eliminación de registros de las bases de datos](#) (en la página 1048)

pdm_logfile: cambio del tamaño de corte de stdlog

pdm_logfile permite cambiar el tamaño de corte de stdlog.x. El corte se produce cuando se escribe un número especificado de bytes. En UNIX, este valor se restablece con cada ejecución de pdm_init. En Windows, los valores se conservan con cada ejecución de pdm_halt y pdm_init.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_logfile [-L|-h]
```

or

```
pdm_logfile [-g -h] [-b bytes]
```

Ejemplo

Para cambiar el corte de los archivos stdlog.x a 500.000 bytes, emita el siguiente comando:

```
pdm_logfile -f STD -b 500000
```

-L

Crea un listado con los cortes actuales.

-q

Ejecuta pdm_logfile en modo silencioso.

-b bytes

Especifica el número de bytes que se escribe antes de que se produzca el corte.

Restricciones

Aunque se puede ejecutar `pdm_load` mientras CA Service Desk Manager está activo, el rendimiento se ve disminuido, por lo que es más aconsejable ejecutar `pdm_load` cuando nadie esté utilizando CA Service Desk Manager.

Importante: En UNIX, `LIBPATH` debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice `pdm_task` para definir `LIBPATH` antes de ejecutar una utilidad. Por ejemplo, indique "`pdm_task pdm_clean_attachments ...`".

pdm_proctor_init: inicio del supervisor en servidores secundarios

Aplicable sólo a UNIX

`pdm_proctor_init` se emplea para iniciar el supervisor en los servidores secundarios. Todos los servidores secundarios se deben haber iniciado antes de iniciar los demonios del servidor principal. Tras detener todos los demonios del servidor principal, utilice `pdm_halt` en el servidor secundario pertinente para detener el supervisor.

Nota: no utilice `pdm_proctor_init` en el servidor primario.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_proctor_init
```

pdm_replace: reemplazo de tablas de bases de datos

`pdm_replace` elimina la tabla de la base de datos de CA Service Desk Manager que se indique y la sustituye por una tabla del archivo temporal especificado con la opción `-f`. Los datos del archivo de entrada son los únicos datos que permanecen en esa tabla después de ejecutar `pdm_replace`. Haga una copia de seguridad de la tabla antes de ejecutar `pdm_replace`.

Nota: como parte de su procesamiento, la utilidad `pdm_replace` cierra primero los daemon (UNIX) o los servicios (Windows).

pdm_replace acepta como entrada archivos de texto, que es el mismo formato de archivo que emplea pdm_userload. Es posible crear un archivo de entrada para la utilidad pdm_replace por medio de la utilidad pdm_extract, pero no se puede emplear como entrada la salida de la utilidad pdm_backup.

Importante: asegúrese de asignar al archivo de entrada un nombre diferente del de la tabla que intente reemplazar. Si reemplaza una tabla llamada, por ejemplo, ca_contacts y asigna al archivo de entrada el nombre ca_contacts.dat, cuando ejecute el comando pdm_replace para señalar al archivo de entrada (ca_contacts.dat), se elimina el archivo tras la ejecución puesto que posee el mismo nombre que la tabla.

Restricciones

- pdm_replace sólo se puede ejecutar en un servidor de CA Service Desk Manager.
- pdm_replace sólo puede ser ejecutado por el usuario con privilegios o el usuario raíz.
- No ejecute pdm_replace cuando algún usuario esté conectado a CA Service Desk Manager.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_replace [-v] -f filename
```

-v

Especifica el modo de detalles.

-f nombre_de_archivo

Especifica un archivo ASCII con el siguiente formato:

```
TABLE nombre_tabla  
nombrecampo1 nombrecampo2. . . nombrecampoN  
{ "valor11", "valor12", . . . "valor1N"}  
{ "valor21", "valor22", . . . "valor2N"}  
.  
.  
.
```

```
{"valorN1", "valorN2", . . . "valorNN"}
```

Se trata del mismo formato de archivo que emplea la utilidad `pdm_userload`. Es posible crear un archivo de entrada para la utilidad `pdm_replace` por medio de la utilidad `pdm_extract`, pero no se puede emplear como entrada la salida de la utilidad `pdm_backup`.

Más información:

[pdm_extract: extracción de datos de las bases de datos](#) (en la página 1019)

[pdm_userload: adición, actualización y eliminación de registros de las bases de datos](#) (en la página 1048)

pdm_restore: restauración de bases de datos

`pdm_restore` detiene CA Service Desk Manager para, acto seguido, eliminar todos los registros de la base de datos de CA Service Desk Manager oportuna y reemplazarlos por registros del archivo especificado con la opción `-f`. Los datos del archivo de entrada son los únicos datos que permanecen en la base de datos de CA Service Desk Manager después de ejecutar `pdm_restore`.

Para crear el archivo de entrada se debe utilizar `pdm_extract` o `pdm_backup`. Si no es así, se le debe dar formato para `pdm_restore`. `pdm_backup` puede hacer una copia de seguridad de los datos ajenos a las bases de datos, y `pdm_restore` también puede restaurar estos datos. Si hay disponibles otras herramientas de copia de seguridad y restauración no se recomienda utilizar `pdm_backup` ni `pdm_restore`.

Nota: como parte de su procesamiento, la utilidad `pdm_restore` cierra primero los `daemon` (UNIX) o los servicios (Windows).

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_restore [-d] [-g] [-n] [-w] [-v] -f filename
```

Restricciones

`pdm_restore` sólo se puede ejecutar en un servidor de CA Service Desk Manager. `pdm_restore` sólo puede ser ejecutado por el usuario con privilegios o el usuario raíz.

Importante: Utilice `pdm_restore` sólo con copias de seguridad completas de las bases de datos creadas con `pdm_backup`, ya que la base de datos actual se elimina y se reemplaza por el archivo de copia de seguridad. No ejecute `pdm_restore` cuando algún usuario esté conectado a CA Service Desk Manager.

-d

Especifica que sólo se restauran los datos de las bases de datos.

-g

Especifica que sólo se restauran los datos que no sean de las bases de datos, Sólo se restauran las ventanas (formularios) y otros datos ajenos a la base de datos.

-n

Especifica que se restaure el archivo `NX.env` si se restauran los datos ajenos a las bases de datos. De forma predeterminada, `NX.env` no se restaura. Recomendamos que el archivo de `NX.env` no sea restaurado a menos que la restauración tenga lugar en el mismo servidor de donde procede la copia de seguridad. Si, por accidente, se restaura un archivo `NX.env` incorrecto, puede afectar a otras bases de datos.

-w

Especifica que se restaure el archivo `web.cfg` si se restauran los datos ajenos a las bases de datos. De forma predeterminada, `web.cfg` no se restaura.

-v

Especifica el modo de detalles.

-f *nombre_de_archivo*

Especifica el archivo de entrada que contiene la copia de seguridad completa creada con `pdm_backup`.

Importante: En UNIX, `LIBPATH` debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice `pdm_task` para definir `LIBPATH` antes de ejecutar una utilidad. Por ejemplo, indique "`pdm_task pdm_clean_attachments ...`".

Más información:

[Restauración de la base de datos](#) (en la página 451)

[pdm_backup: escritura de bases de datos en archivos ASCII](#) (en la página 1007)

[pdm_userload: adición, actualización y eliminación de registros de las bases de datos](#) (en la página 1048)

pdm_status: visualización del estado de demonios o procesos

pdm_status muestra el estado de todos los demonios (UNIX) o procesos (Windows) de CA Service Desk Manager del sistema en el que se ejecute el comando.

La salida se muestra con este formato:

DAEMON		STATUS	HOST	PID	SLUMP	CONNECT	TIME

Agente anthill		En ejecución	anthill	455	Mar	Feb	17
17:55:12							
Ddict_rd	(ddictrd)	Completado	anthill				
Data Dictionary	(ddictbuild)	Completado	anthill				
...							
User Validation	(boplgln)	En ejecución	anthill	456	Mar	Feb	17
17:55:21							

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_status
```

pdm_task: definición de variables de entorno

Aplicable sólo a UNIX

La utilidad pdm_task define variables de entorno para los comandos que carecen de contenedores. Por ejemplo, el comando pdm_task se antepone al comando report en la misma línea de comandos **sólo** cuando se invoca el comando por medio de una secuencia de comandos o de la línea de comandos. Si se emite el comando report desde un menú, no hace falta incluir pdm_task, ya que la propia aplicación define todas las variables de entorno.

Nota: No se pueden generar informes desde la línea de comandos de los clientes.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_task comando
```

comando

Especifica un comando que carece de contenedor y que, por lo tanto, no define automáticamente las variables de entorno. Si desea obtener más información sobre la emisión de pdm_task con comandos, consulte report: generación de informes (see page 1055).

pdm_text_cmd: interfaz de la línea de comandos de Text API

pdm_text_cmd es la interfaz de la línea de comandos de Text API, que sirve para crear y actualizar diversos objetos como, por ejemplo, solicitudes, órdenes de cambio, incidencias, activos y contactos.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_text_cmd -t table {-u from_userid -p from_persid} [-o operation] [-f input file] [-T timeout] [-h]
```

-t *table*

(Obligatorio) Especifica la tabla que se debe procesar. El nombre de *tabla* puede ser uno de los siguientes valores (no se distingue entre mayúsculas y minúsculas):

- Activo
- Contacto
- Cambiar
- Incidencia
- Solicitud

Nota: consulte en la sección [OPTIONS] del archivo text_api.cfg la lista completa de nombres de tabla válidos.

-u *from_userid* | **-p** *from_persid*

(Una opción es obligatoria) Identifica el contacto para esta operación:

-u *from_userid*

Identifica el contacto con el valor de ID de usuario.

-p *from_persid*

Identifica el contacto con el identificador de objeto exclusivo para el registro de contacto. *from_persid* debe tener la forma **cnt:xxxx. xxxx** es el ID persistente del objeto.

Nota: el valor especificado con esta opción se agrega al final de la entrada para el comando `pdm_text_cmd` mediante la palabra clave apropiada, `%FROM_USERID` o `%FROM_PERSID`.

-o *operation*

Especifica la operación que se debe realizar. El valor de *operation* debe ser uno de los siguientes valores (no se distingue entre mayúsculas y minúsculas):

- **NEW:** crea un objeto. Se trata del valor predeterminado en caso de que no se especifique ninguna operación.
- **UPDATE | UPD:** si no se encuentra el objeto, se crea y, si se encuentra, se actualiza.
- **UPDATE_ONLY | UPDO:** si se encuentra el objeto, se actualiza; de lo contrario, no se realiza ninguna acción.

Tanto **UPDATE** como **UPDATE_ONLY** requieren que se use la palabra clave `%SEARCH` en la entrada del comando. Sólo se puede realizar una operación cada vez que se invoque `pdm_text_cmd`.

-f *input_file*

Especifica la ruta completa al archivo que se debe procesar, que es un archivo de texto que contiene comandos de Text API válidos. Si se omite este parámetro, se utilizan los comandos de STDIN. El Text API utiliza el siguiente formato básico para la entrada:

%palabra_clave=valor

Puede emitir varios comandos dentro de la entrada si separa la solicitud de comandos con al menos cinco símbolos de porcentaje (%%%%%).

Nota: Para obtener más información sobre palabras clave válidas y sobre el formato de la entrada en Text API, consulte el archivo `text_api.cfg`. Para obtener más información, consulte *Uso de Text API*. (see page 473)

-T *timeout*

Especifica el número de segundos que se espera a que se produzca la respuesta del servidor antes de que se dé por agotado el tiempo de espera. El valor predeterminado es 30 segundos.

Nota: pdm_text_cmd muestra las respuestas basadas en texto y recibidas de Text API, que incluyen mensajes de error o de confirmación, así como el texto original enviado mediante la API para su procesamiento. pdm_text_cmd devuelve cero si el comando se ejecuta correctamente sin advertencias ni errores, o bien devuelve uno si se ejecuta correctamente pero con advertencias. Si se devuelve cualquier otro valor, significa que se ha producido algún error.

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

Ejemplos de entrada

pdm_text_cmd es la interfaz de la línea de comandos de Text API, que se puede utilizar para crear y actualizar diferentes objetos como, por ejemplo, solicitudes, órdenes de cambios, incidencias, activos o contactos.

Ejemplo: utilización de un archivo de entrada para crear una incidencia

El ejemplo siguiente demuestra cómo utilizar un archivo de entrada pdm_text_cmd para crear una incidencia:

```
%DESCRIPTION=Ésta es mi prueba.  
%PRIORITY=3
```

Para procesar este archivo (suponiendo que la ruta completa sea c:\input.txt), se emite el comando siguiente:

```
pdm_text_cmd -t Issue -u user01 -f c:\input.txt
```

Ejemplo: utilización de un archivo de entrada para actualizar una incidencia

En el siguiente ejemplo se muestra un archivo de entrada para actualizar la incidencia 123 a la prioridad 2:

```
%SEARCH=ISSUE_ID
%ISSUE_ID=123
%PRIORITY=2
```

Para procesar este archivo (suponiendo que la ruta completa sea c:\update.txt), se emite el comando siguiente:

```
pdm_text_cmd -t Issue -o UPDATE_ONLY -u user01 -f c:\update.txt
```

Ejemplo: utilización de un archivo de entrada para crear varias solicitudes.

El ejemplo siguiente ilustra la creación de varias solicitudes con un solo archivo de entrada. Este comando puede resultar útil para crear datos de prueba en un sistema de prueba.

```
%DESCRIPTION=Ésta es la prueba 1.
%PRIORITY=3
%%%%
%DESCRIPTION=Ésta es la prueba 2.
%PRIORITY=2
%%%%
%DESCRIPTION=Ésta es la prueba 3.
%PRIORITY=Ninguno
```

Para procesar este archivo (suponiendo que la ruta completa sea c:\testdata.txt), se emite el comando siguiente:

```
pdm_text_cmd -t Request -u user01 -f c:\testdata.txt
```

pdm_uconv--Conversión de un conjunto de caracteres local a UTF-8

La utilidad pdm_uconv le ayuda a convertir datos de versiones anteriores de CA Service Desk Manager o integraciones con otros productos de CA. El uso más común de esta utilidad es convertir de un conjunto de caracteres local a UTF-8 y viceversa.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_uconv -h [-V] [-s] [-v] [-l | --list-code  
| --default-code | -L] [--cannon] [-x] [--to-callback | -c] [--from-callback | -  
i] [--fallback | --no-fallback] [-b] [-f] [--t] [--add-signature] [--remove-  
signature] [-o] [file ...]
```

-h

Abre el menú Ayuda.

-V

Imprime la versión de programa.

-s

Utiliza operación silenciosa y suprime mensajes.

-v

Muestra la información sobre el progreso de la utilidad.

-l

Enumera toda la codificación disponible. Los siguientes valores son válidos:

--list-code

Enumera solamente la codificación especificada.

--default-code

Enumera solamente la codificación predeterminada.

-L

Enumera todos los transliteradores disponibles.

--cannon

Imprime la lista en el formato de cnvtrs.txt(5).

-x

Ejecuta el progreso a través de la transliteración.

devolución de llamada --to-callback

Utiliza devolución de llamada en la codificación de destino.

-c

Omite caracteres no válidos del resultado.

devolución de llamada --from-callback

Utiliza devolución de llamada en la codificación original.

-i

Omite secuencias no válidas en la entrada.

devolución de llamada --callback

Utiliza devolución de llamada en las dos codificaciones.

-b

Especifica el tamaño de bloque.

Valor predeterminado: 4096

-- fallback

Utiliza asignación de reserva.

--no-fallback

No utiliza asignación de reserva.

-f

Establece la codificación original.

-t

Establece la codificación de destino.

--add-signature

Agrega un carácter de firma de Unicode de U+FEFF (BOM).

--remove-signature

Quita un carácter de firma de Unicode de U+FEFF (BOM).

-o

Escribe la salida en el archivo.

Ejemplos:

Del conjunto de caracteres local a UTF-8

```
pdm_uconv -t utf-8 inputfile.txt > outputfile.txt
```

Del conjunto de caracteres específico (iso-2022-jp) a UTF-8

```
pdm_uconv -f iso-2022-jp -t utf-8 inputfile.txt > outputfile.txt
```

De UTF-8 al conjunto de caracteres local

```
pdm_uconv -f utf-8 inputfile.txt > outputfile.txt
```

De UTF-8 al conjunto de caracteres específico

```
pdm_uconv -f utf-8 -t iso-2022-jp inputfile.txt > outputfile.txt
```

La utilidad pdm_uconv tiene las siguientes devoluciones de llamada válidas:

- substitute
- skip
- stop
- escape
- escape-icu
- escape-java
- escape-c
- escape-xml
- escape-xml-hex
- escape-xml-dec
- escape-unicode

pdm_userload: adición, actualización y eliminación de registros de las bases de datos

pdm_userload actualiza la base de datos de CA Service Desk Manager con el archivo de entrada que se especifique.

Importante: antes de ejecutar pdm_userload, realice siempre una copia de seguridad de la base de datos oportuna.

Cada vez que se carguen partes (como incidencias o solicitudes), el número de parte debe incluir un prefijo o un sufijo exclusivo en la cadena. CA Service Desk Manager considera este número como una cadena de caracteres, no como un número secuencial, y, por ello, no puede garantizar la asignación de un número exclusivo a los partes cargados. Mientras se asigne un prefijo o un sufijo exclusivo con awk u otro procesador de textos, no obstante, es posible cargar partes sin que CA Service Desk Manager escriba encima de los números asignados con anterioridad.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_userload [-a] [-c] [-h] [-r] [-v] [-u] [-m] -f filename
```


Formato del archivo de entrada

Las entradas del archivo de entrada siguen este formato:

```
TABLE nombre_tabla
nombrecampo1 nombrecampo2. . . nombrecampoN
{ "valor11", "valor12", . . . "valor1N"}
{ "valor21", "valor22", . . . "valor2N"}
.
.
.
{ "valorN1", "valorN2", . . . "valorNN"}
```

table_name es el nombre de la tabla que se pretende cargar tal como aparece en el archivo del esquema de la base de datos de CA Service Desk Manager, que se ubica en \$NX_ROOT/site/schema.sch (UNIX) o en *directorio-instalación*\site\schema.sch (Windows), donde \$NX_ROOT o *directorio-instalación* es el directorio en el que se instaló CA Service Desk Manager.

-f filename

Especifica un archivo ASCII de entrada.

-a

Actualiza todos los registros existentes aunque coincida más de un registro existente con un solo registro de entrada. Sin esta opción, se rechazan los registros de entrada que coincidan con más de un registro existente.

Importante: utilice esta opción con cuidado.

-c

Coteja el archivo de entrada con la base de datos y se limita a informar sobre las actualizaciones que habría que realizar (no las lleva a cabo).

-r

Elimina los registros de la base de datos que coincidan con los registros de entrada. La opción -a se puede utilizar junto con la opción -r.

Nota: Antes de ejecutar pdm_userload con esta opción, realice una copia de seguridad de la base de datos. Una vez que se eliminen los registros antiguos de la base de datos, es preciso restaurar la base de datos de CA Service Desk Manager con esta copia de seguridad para recuperar alguno de ellos.

-v

Especifica el modo de detalles.

-u

Actualiza los registros existentes pero no inserta ningún registro nuevo en la base de datos.

-m

Hace referencia a la actualización masiva. Se especifica cuando se emplea pdm_userload para agregar o eliminar un número elevado de registros. Esta opción suprime todas las notificaciones de actualización de los clientes y envía un mensaje de actualización de la caché de la tabla pertinente cuando pdm_userload termina de procesarla.

-x

Usa formatos de entrada numéricos adaptados a la configuración regional.

-t

Especifica el nombre o UUID de cliente para asociar todos los datos cargados con el cliente especificado. Este argumento es válido solamente cuando se instala el multicliente.

Pdm_userload admite nuevos argumentos en la instrucción TABLE, "Truncate" y "NoNewID". Estos argumentos se especifican en una opción entre paréntesis opcional después del nombre de tabla. Por ejemplo:

```
TABLE Call_Req (TRUNCATE, NONEWID)
```

Truncate

Hace que pdm_userload emita un comando TRUNCATE específico de la base de datos para la tabla antes de cargar los datos. Además, se obliga a la lógica de pdm_userload a utilizar lógica de sólo inserción independientemente de los argumentos de la línea de comandos, ya que todos los registros son nuevos.

NoNewID

Hace que pdm_userload utilice el valor de ID del archivo de control de entradas para nuevas filas en la tabla, en vez de generar un nuevo ID para los datos insertados (la lógica predeterminada de la opción -i de pdm_userload).

Restricciones

Aunque se puede ejecutar pdm_userload mientras CA Service Desk Manager está activo, el rendimiento se ve disminuido, por lo que es más aconsejable ejecutar pdm_userload cuando nadie esté utilizando CA Service Desk Manager.

Más información:

[pdm_backup: escritura de bases de datos en archivos ASCII](#) (en la página 1007)

[pdm_replace: reemplazo de tablas de bases de datos](#) (en la página 1037)

[pdm_restore: restauración de bases de datos](#) (en la página 1039)

pdm_webstat: devolución de estadísticas de uso Web

Utilice pdm_webstat para devolver estadísticas sobre los usuarios y las sesiones de CA Service Desk Manager relativas a uno o más de los procesos de los motores Web. El comando pdm_webstat muestra los valores relacionados con las sesiones acumuladas, con la mayor cantidad de sesiones simultáneas y con las sesiones activas en el momento. Asimismo, se proporciona información, si se desea, sobre usuarios concretos.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_webstat [-r] [-d | -D] [-i] [-t timeout] [-p webengine process] [-n] [-h]
```

-r

Especifica el modo de texto sin procesar, sin títulos ni ningún otro formato. Dentro de la salida de un solo proceso de motor Web, no hay ningún salto de línea pero la salida de cada proceso siempre empieza en una línea nueva.

El modo de texto sin procesar muestra los datos exactamente en el mismo orden que cuando se utiliza pdm_webstat sin la opción -r. Este modo se emplea si los datos resultantes se pretenden usar en hojas de cálculo u otros tipos de informe. Por ejemplo, la sintaxis siguiente:

```
pdm_webstat -r
```

muestra el siguiente resultado:

```
10/11/2005 10:31:49 web:local:0 12 4 2
10/11/2005 10:31:49 web:local:1 9 2 2
```

-d

Especifica una salida detallada que muestra las sesiones de los usuarios. La opción -d muestra todas las sesiones actuales con el formato *ID_usuario@dirección_IP*. Si alguna sesión aparece sin ningún ID de usuario, suele indicar que aún no se ha iniciado la sesión. Por ejemplo, la sintaxis siguiente:

```
pdm_webstat -d
```

muestra el siguiente resultado:

```
PDM_Webstat: invocado el 11/10/05 10:27:31
```

```
=====
Informe del motor Web: web:local:0
=====
```

```
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
    @192.168.1.16
    usery@192.168.1.20
=====
```

```
Informe del motor Web: web:local:1
=====
```

```
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
    SrvcPlus@192.168.1.14
    userx@192.168.1.8
=====
```

-D

Proporciona una salida más detallada con fines de depuración. Sólo se debe especificar esta opción cuando lo solicite de forma explícita el soporte técnico de CA. Agrega información interna sobre las sesiones a la salida detallada. Por ejemplo, la sintaxis siguiente:

```
pdm_webstat -D
```

muestra el siguiente resultado:

```
PDM_Webstat: Invocado el 10/11/07 10:28:10
```

```
=====
Informe del motor Web: web:local:0
=====
```

```
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
  @192.168.1.16           SessionStat  1
  userx@192.168.1.20      SessionStat  5
=====
```

```
Informe del motor Web: web:local:1
=====
```

```
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
  SrvcPlus@192.168.1.14   SessionStat  7
  userx@192.168.1.8       SessionStat 13
=====
```

-i

Especifica el intervalo en segundos que transcurre entre informes sucesivos. Cuando se especifica el argumento `-i`, `pdm_webstat` se ejecuta de manera continua. El comando `pdm_webstat` emite su informe en el formato solicitado por otros argumentos, espera el intervalo especificado, y emite nuevamente el informe. Con la opción `-i`, `pdm_webstat` sólo finaliza cuando se cancela de forma explícita, por lo general, pulsando las teclas `Ctrl+C`. Por ejemplo, la sintaxis siguiente:

```
pdm_webstat -i 5 -p web:local -r
```

muestra el siguiente resultado:

```
21/09/07 16:27:25 web:local 14 10 6
21/09/07 16:27:30 web:local 17 10 9
21/09/07 16:27:35 web:local 18 10 10
21/09/07 16:27:41 web:local 21 13 13
```

-t timeout

Especifica un valor de tiempo de espera en segundos. Este parámetro hace que `pdm_webstat` espere una respuesta durante el número de segundos indicado antes de proceder a la finalización. El valor predeterminado es 30 segundos.

-p webengine_process

Especifica el nombre de proceso del motor Web sobre el que se desea elaborar el informe. De forma predeterminada, se realizan informes de todos los procesos de los motores Web. El nombre de proceso (también llamado nombre de slump) es el mismo nombre que se vería en la salida de la utilidad slstat y siempre comienza por "web:".

-n

Suprime la entrada de registro normal de cada uno de los motores Web reflejados en los informes. De forma predeterminada, se crea una entrada de registro donde se resumen los datos de cada uno de ellos.

Nota: Si no se especifica ningún parámetro, pdm_webstat muestra de forma predeterminada un resumen de los datos correspondientes a todos los procesos en ejecución.

pdm_webstat devuelve cero si el comando se ejecuta correctamente y cualquier otro valor si se produce algún error (por ejemplo, si se agota el tiempo de espera o si no hay ningún proceso del motor Web activo).

Ejemplo: salida de pdm_webstat cuando no se especifican parámetros

En el siguiente ejemplo se muestra la salida de pdm_webstat cuando se ejecuta sin parámetros:

```
PDM_webstat: Invocado el 10/11/07 10:28:42
```

```
=====
Informe del motor web: web:local:0
=====
```

```
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
=====
```

```
Informe del motor web: web:local:1
=====
```

```
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
```

Importante: En UNIX, LIBPATH debe estar definido antes de ejecutar varias utilidades CA Service Desk Manager. Utilice *pdm_task* para definir LIBPATH antes de ejecutar una utilidad. Por ejemplo, indique "pdm_task pdm_clean_attachments ...".

report: generación de informes

Aplicable sólo a UNIX

El programa report permite generar informes desde la línea de comandos del servidor. Para emitir el comando report en la línea de comandos o en una secuencia de comandos, es preciso incluir el comando pdm_task, que configura las variables de entorno para los comandos que carecen de contenedores. Escriba pdm_task con el comando report en la misma línea de comandos *sólo* cuando se invoque el comando por medio de un script o de la línea de comandos. Si se emite el comando report desde un menú, no hace falta incluir pdm_task, ya que la propia aplicación define todas las variables de entorno.

Sintaxis

Este comando tiene el formato siguiente:

```
pdm_task report [-h] [-e] [-f] [-F ffstring] [-p pagelength] filename [ command  
line arguments]
```

-e

Repite la secuencia de comandos compilada (con fines de depuración).

-f

Usa avances de página entre las páginas.

-F ffstring

Define la cadena de avance de página opcional.

-p pagelength

Define la longitud de las páginas. La longitud predefinida de las páginas es de 66.

filename

La plantilla del informe. Si el comando report no se ejecuta en el mismo directorio donde se ubica el archivo de plantillas, escriba la ruta completa al archivo. El comando envía la salida como salida estándar (stdout).

command line arguments

Especifica los parámetros que recibe la plantilla del informe. Si el informe está diseñado para aceptar argumentos de línea de comandos, es necesario escribir uno por cada parámetro existente en la plantilla. Si el argumento está vacío, escriba la cadena de valor nulo.

Por ejemplo, el siguiente comando suministra los argumentos de línea de comandos Saura, Julia y L. La plantilla del informe requiere estos tres parámetros para generar el Informe de contactos afectados.

Por ejemplo, escriba lo siguiente:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt
```

En el siguiente ejemplo, Julia Saura no tiene ningún segundo nombre:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt Saura Julia "
```

rpt_srv: generación de informes

Válido solamente en Windows

El programa report permite generar informes desde la línea de comandos del servidor. Para emitir el comando report en la línea de comandos o en una secuencia de comandos, es preciso incluir el comando pdm_task, que configura las variables de entorno para los comandos que carecen de contenedores. Escriba pdm_task con el comando report en la misma línea de comandos sólo cuando se invoque el comando por medio de un script o de la línea de comandos. Si se emite el comando report desde un menú, no hace falta incluir pdm_task, ya que la propia aplicación define todas las variables de entorno.

Sintaxis

Este comando tiene el formato siguiente:

```
rpt_srv -m [-h] [-e] [-f] [-F ffstring] [-p pagelength] [-C] [-B] filename [
command line arguments]
```

-m

Significa que el informe se ejecuta manualmente en la línea de comandos.

-e

Repite la secuencia de comandos compilada (con fines de depuración).

-f

Usa avances de página entre las páginas.

-F ffstring

Define la cadena de avance de página opcional.

-p pagelength

Define la longitud de las páginas. La longitud predefinida de las páginas es de 66.

-C

Cambios que codifican de UTF-8 a otro conjunto de caracteres. El resultado predeterminado es UTF-8.

Ejemplo: Para convertir el resultado a JIS, puede ejecutar "-C iso-2022-jp"

Ejemplo: Para codificar al conjunto de caracteres nativo del sistema operativo, utilice "PREDETERMINADO" o "NATIVO".

-B

Suprime la marca de orden de bytes si la variable NX_ADD_UTF8_BYTE_ORDER_MARK está establecida.

La opción NX_ADD_UTF8_BYTE_ORDER_MARK es una firma en un archivo. Permite a los editores que admiten UTF-8 mantener la integridad de UTF-8 del archivo.

Nota: Sólo es necesario para datos que no son ASCII. Si no está instalado, el comportamiento predeterminado omite la marca de orden de bytes (BOM). Si está instalado, establézcalo en "1" o "Sí".

filename

Especifica la plantilla del informe. Si el comando report no se ejecuta en el mismo directorio donde se ubica el archivo de plantillas, escriba la ruta completa al archivo. El comando envía la salida como salida estándar (stdout).

command line arguments

Especifica los parámetros que recibe la plantilla del informe. Si el informe está diseñado para aceptar argumentos de línea de comandos, es necesario escribir uno por cada parámetro existente en la plantilla. Si el argumento está vacío, escriba la cadena de valor nulo.

Por ejemplo, el siguiente comando suministra los argumentos de línea de comandos Saura, Julia y L.. La plantilla del informe requiere estos tres parámetros para generar el Informe de contactos afectados.

Por ejemplo, introduzca el siguiente comando:

```
rpt_srv -m c:\reports\affected.rpt Smith Jane L
```

En el siguiente ejemplo, Julia Saura no tiene ningún segundo nombre:

```
rpt_srv -m c:\reports\affected.rpt Smith Jane "
```

uniconv: inicio de daemon de conversor de eventos de CA NSM en UNIX

Aplicable sólo a UNIX

Cuando CA Service Desk Manager se integra con CA NSM, se puede utilizar uniconv para enviar datos sobre eventos genéricos a fin de filtrar los daemon de CA Service Desk Manager. uniconv se utiliza en acciones de mensaje de la gestión de eventos de CA NSM.

Sintaxis

Este comando tiene el formato siguiente:

```
uniconv -h &opnode -e &'text' [-n &
nodeid] [-u &userid] [-d &datem] [-t &
time']
```

Restricciones

uniconv se debe ejecutar desde \$NX_ROOT/bin en UNIX. El sitio debe estar integrado con CA NSM para poder servirse de esta utilidad.

-h &opnode

Especifica el nombre del nodo del equipo en el que se ejecuta uniconv (obligatorio).

-e &'text'

Especifica el texto completo del mensaje (obligatorio).

-n &nodeid

Especifica el nombre del nodo desde el que se origina el mensaje (obligatorio).

-u &userid

Especifica el ID de inicio de sesión de la persona que da origen al mensaje.

-d &datem

Especifica la fecha del sistema en formato *dd/mm/yy*.

-t &'time'

Especifica la hora del sistema.

Apéndice D: Grupos de formularios

Esta sección contiene los siguientes temas:

[Grupo de formularios de cliente](#) (en la página 1059)

[Grupo de formularios de empleado](#) (en la página 1060)

[Grupo de formularios de analista](#) (en la página 1062)

Grupo de formularios de cliente

Los siguientes formularios Web se incluyen en los grupos de formularios de cliente:

- about.html
- bin_form_np.html
- chg_lr.html
- cr_lr.html
- detail_iss.html
- detail_issalg.html
- detail_KD.html
- generic.html
- home.html
- iss_lr.html
- issue_status_change.html
- list_iss.html
- list_isscat.html
- list_KD.html
- menu_frames.html
- std_body.html
- std_body_site.html
- std_footer.html
- std_footer_site.html
- std_head.html
- std_header.html
- std_head_site.html

Grupo de formularios de empleado

Los siguientes formularios Web se incluyen en los grupos de formularios de empleado:

- about.html
- bin_form_np.html
- buttons.html
- change_status_change.html
- chg_lr.html
- cr_lr.html
- detail_alg.html
- detail_chg.html
- detail_chgalg.html
- detail_cr.html
- detail_in.html
- detail_KD.html
- generic.html
- home.html
- iss_lr.html
- list_chg.html
- list_chgcat.html
- list_cr.html
- list_in.html
- list_KD.html
- list_pcat.html
- list_pcat_cr.html
- list_pcat_in.html
- menu_frames.html

- request_status_change.html
- show_error.html
- std_body.html
- std_body_site.html
- std_footer.html
- std_footer_site.html
- std_head.html
- std_header.html
- std_head_site.html

Grupo de formularios de analista

Los siguientes formularios Web se incluyen en los grupos de formularios de analista:

A

- about.html
- acctyp_role_tab.html
- acctyp_web_auth_tab.html
- acctyp_wsp_tab.html
- admin_empty.html
- admin_main_role.html
- admin_tab_dflt.html
- admin_tree.html
- attmnt_content_tab.html
- attmnt_fields.html
- attmnt_permissions_tab.html
- attmnt_upload_popup.html
- att_mgs_event.html
- att_stype_event.html
- aty_chg_ntfr_tab.html
- aty_chg_svy_tab.html
- aty_cr_ntfr_tab.html
- aty_cr_svy_tab.html
- aty_iss_ntfr_tab.html
- aty_iss_svy_tab.html
- aty_kdComment_ntfr_tab.html
- aty_kd_ntfr_tab.html
- aty_mgs_ntfr_tab.html

B

- bhvtpl_todo_tab.html
- bhvtpl_trans_info_tab.html
- bin_form_np.html

C

- cancel.html
- cancel_empty.html
- category_content_tab.html
- category_permissions_tab.html
- chgcat_auto_assignment_tab.html
- chgcat_prptpl_tab.html
- chgcat_wftpl_tab.html
- chg_accumulate.html
- chg_causedreq_tab.html
- chg_close_all_child.html
- chg_expedite.html
- chg_lr.html
- chg_relchg_tab.html
- chg_relreq_tab.html
- cia_bmhier_tab.html
- cia_export_bmhier.html
- cia_export_nr.html
- cia_nr_tab.html
- cia_pwd_tab.html
- cia_sync_stat.html
- cnote_tracker.html
- cnt_addr_tab.html
- cnt_auto_assignment_tab.html
- cnt_env_tab.html
- cnt_grp_tab.html
- cnt_mem_tab.html
- cnt_notif_tab.html
- cnt_org_tab.html
- cnt_rem_tab.html
- cnt_role_tab.html
- cr_attach_chg.html
- cr_close_all_child.html
- cr_detach_chg.html

- cr_lr.html
- cr_relreq_tab.html

S

- dcon_constraint_tab.html
- dcon_sql_tab.html
- detail.template
- detail_acctyp.html
- detail_act_type_assoc.html
- detail_ADMIN_TREE.html
- detail_alg.html
- detail_arcpur_rule.html
- detail_asset.html
- detail_atev.html
- detail_atomic_cond.html
- detail_atmnt_edit.html
- detail_atmnt_error.html
- detail_atmnt_folder.html
- detail_atmnt_ro.html
- detail_attr_alias.html
- detail_aty.html
- detail_audlog.html
- detail_bhvtpl.html
- detail_bmcls.html
- detail_bmhier.html
- detail_bmrep.html
- detail_BU_TRANS.html
- detail_ca_cmpny.html
- detail_chg.html
- detail_chgalg.html
- detail_chgcat.html
- detail_chgstat.html
- detail_chgtype.html
- detail_CI_ACTIONS.html

- detail_CI_ACTIONS_ALTERNATE.html
- detail_CI_DOC_TEMPLATES.html
- detail_CI_STATUSES.html
- detail_CI_WF_TEMPLATES.html
- detail_cmth.html
- detail_cnote.html
- detail_cnt.html
- detail_cost_cntr.html
- detail_country.html
- detail_cr.html
- detail_crs.html
- detail_crsq.html
- detail_cr_prptpl.html
- detail_ctab.html
- detail_ctimer.html
- detail_ctp.html
- detail_dcon.html
- detail_dept.html
- detail_dmn.html
- detail_doc_rep.html
- detail_DOC_VERSIONS.html
- detail_EBR_ACRONYMS.html
- detail_EBR_LOG.html
- detail_EBR_NOISE_WORDS.html
- detail_EBR_SYNONYMS_ADM.html
- detail_event_log.html
- detail_evt.html
- detail_fmgrp.html
- detail_grc.html
- detail_g_cnt.html
- detail_g_loc.html
- detail_g_org.html
- detail_g_prod.html

- detail_g_qname.html
- detail_g_srvrs.html
- detail_g_tblmap.html
- detail_g_tblrule.html
- detail_help_set.html
- detail_hier_edit.html
- detail_hier_ro.html
- detail_ical_event_template.html
- detail_imp.html
- detail_in.html
- detail_iss.html
- detail_issalg.html
- detail_isscat.html
- detail_issstat.html
- detail_iss_wf.html
- detail_kc.html
- detail_KCAT.html
- detail_KD.html
- detail_KD_FILE.html
- detail_KD_QA.html
- detail_KD_SAVE_AS.html
- detail_KD_TASK.html
- detail_KD_TASK_cancel_rework.html
- detail_KD_TASK_retire.html
- detail_KD_template.html
- detail_KEIT_TEMPLATES.html
- detail_KT_ACT_CONTENT.html
- detail_KT_BLC.html
- detail_KT_FILE_TYPE.html
- detail_KT_FLG_TYPE.html
- detail_ldap.html
- detail_ldap_group.html
- detail_loc.html

- detail_LONG_TEXTS.html
- detail_lr_ro.html
- detail_macro.html
- detail_macro_type.html
- detail_menu_bar.html
- detail_menu_tree_name.html
- detail_mfrmod.html
- detail_mgs.html
- detail_mgsalg.html
- detail_mgsstat.html
- detail_NOTIFICATION.html
- detail_no_contract_sdsc.html
- detail_nr.html
- detail_nrf.html
- detail_nr_com.html
- detail_ntfl.html
- detail_ntfm.html
- detail_ntfr.html
- detail_options.html
- detail_org.html
- detail_O_COMMENTS.html
- detail_O_EVENTS.html
- detail_pcat.html
- detail_perscnt.html
- detail_position.html
- detail_pr.html
- detail_prefs.html
- detail_pri.html
- detail_prod.html
- detail_projex.html
- detail_prptpl.html
- detail_prpval.html
- detail_prpval_rule.html

- detail_prp_edit.html
- detail_QUERY_POLICY.html
- detail_rc.html
- detail_response.html
- detail_role.html
- detail_role_go_form.html
- detail_rptmeth.html
- detail_rrf.html
- detail_rss.html
- detail_sapolicy.html
- detail_saprobtyp.html
- detail_sdsc.html
- detail_sdsc_map.html
- detail_seq.html
- detail_sev.html
- detail_site.html
- detail_slatpl.html
- detail_svr_aliases.html
- detail_svr_zones.html
- detail_state.html
- detail_svc_contract.html
- detail_svy_atpl.html
- detail_svy_qtpl.html
- detail_svy_tpl.html
- detail_tab.html
- detail_tenant.html
- detail_tenant_group.html
- detail_tskstat.html
- detail_tskty.html
- detail_tspan.html
- detail_typecnt.html
- detail_tz.html
- detail_urg.html

- detail_USP_PREFERENCES.html
- detail_usp_servers.html
- detail_vpt.html
- detail_web_form.html
- detail_wf.html
- detail_wftpl.html
- detail_wrkshft.html
- dmn_dcon_tab.html
- edit_prop_dyn.html
- ed_image_pane.html
- evt_action_info.html
- evt_config_info.html

G

- generic.html
- get_comment.html
- g_profile_browser.html
- g_profile_browser2.html
- g_profile_browser3.html
- g_profile_browser_frameset.html
- g_profile_jump.html
- g_profile_scratchpad.html

A

- hierload_admin_tree.html
- hierload_KCAT.html
- hiersel_admin_tree.html
- hiersel_KCAT.html
- hourglass.html
- html_editor_create_change_order.html
- html_editor_create_ticket.html
- html_editor_frames.html
- html_editor_insert_image.html
- html_editor_insert_link.html

- html_editor_insert_table.html
- html_editor_tabs.html
- html_editor_toolbar.html

No acepto

- insert_iss_wf.html
- insert_wf.html
- in_relreq_tab.html
- isscat_auto_assignment_tab.html
- isscat_prptpl_tab.html
- isscat_wftpl_tab.html
- issue_status_change.html
- iss_accumulate.html
- iss_close_all_child.html
- iss_custfld_tab.html
- iss_expedite.html
- iss_lr.html
- iss_reliss_tab.html
- iss_resol_tab.html

K

- kd_action_forward.html
- kd_action_publish.html
- kd_action_reject.html
- kd_action_unpublish.html
- kd_action_unretire.html
- kd_attachments_tab.html
- kd_attributes_tab.html
- kd_categories_tab.html
- kd_content_tab.html
- kd_file_prop_tab.html
- kd_permissions_tab.html
- kd_qa_attributes_tab.html
- kd_qa_content_tab.html

- keit_tmpl_export_fields_tab.html
- keit_tmpl_export_filter_tab.html
- keit_tmpl_import_settings_tab.html
- keit_tmpl_name_tab.html
- kt_admin_attachments.html
- kt_admin_automated_policies.html
- kt_admin_document_settings.html
- kt_admin_faq_options.html
- kt_admin_general_settings.html
- kt_admin_integration.html
- kt_admin_knowledge.html
- kt_admin_parse_settings.html
- kt_admin_report_card.html
- kt_admin_search_config_cr.html
- kt_admin_search_config_iss.html
- kt_admin_search_options.html
- kt_admin_survey_settings.html
- kt_admin_workflow_settings.html
- kt_architect.html
- kt_architect2.html
- kt_architect3.html
- kt_architect_delete_KCAT.html
- kt_architect_delete_KD.html
- kt_architect_frameset.html
- kt_architect_init.html
- kt_architect_javascript.html
- kt_architect_KCATs.html
- kt_architect_KCAT_path.html
- kt_architect_KDs.html
- kt_dtbuilder.html
- kt_dtbuilder2.html
- kt_dtbuilder3.html
- kt_dtbuilder_frameset.html

- kt_dtbuilder_node.html
- kt_dtbuilder_prompt_window.html
- kt_dtbuilder_save_dialog_window.html
- kt_dtbuilder_save_tree_form.html
- kt_dtbuilder_tree.html
- kt_email_document.html
- kt_faq_tree.html
- kt_main.html
- kt_main2.html
- kt_main3.html
- kt_main_role.html
- kt_permissions.html

L

- list.template
- list_acctyp.html
- list_act_type_assoc.html
- list_alg.html
- list_all_fmgrp.html
- list_all_lr.html
- list_architect_KDs.html
- list_architect_KDs_Pref.html
- list_arcpur_hist.html
- list_arcpur_rule.html
- list_atev.html
- list_atomic_cond.html
- list_atmnt.html
- list_attr_alias.html
- list_aty.html
- list_audlog.html
- list_bmcls.html
- list_bmhier.html
- list_bmrep.html
- list_bm_task.html

- list_bool.html
- list_ca_cmpny.html
- list_ca_logical_asset.html
- list_chg.html
- list_chgalg.html
- list_chgcat.html
- list_chgsched.html
- list_chgsched_config.html
- list_chgstat.html
- list_chgtype.html
- list_CI_ACTIONS.html
- list_CI_ACTIONS_ALTERNATE.html
- list_CI_DOC_TEMPLATES.html
- list_CI_STATUSES.html
- list_CI_WF_TEMPLATES.html
- list_cmth.html
- list_cnote.html
- list_cnt.html
- list_cost_cntr.html
- list_country.html
- list_cr.html
- list_crs.html
- list_crsq.html
- list_crs_cr.html
- list_crs_in.html
- list_crs_pr.html
- list_crt.html
- list_cr_kt.html
- list_ctab.html
- list_ctimer.html
- list_ctp.html
- list_dcon.html
- list_dept.html

- list_dmn.html
- list_DOC_VERSIONS.html
- list_EBR_ACRONYMS.html
- list_EBR_LOG.html
- list_EBR_NOISE_WORDS.html
- list_EBR_SYNONYMS_ADM.html
- list_event_log.html
- list_evt.html
- list_evtdly.html
- list_grc.html
- list_grpmem.html
- list_g_chg_queue.html
- list_g_cnt.html
- list_g_cr_queue.html
- list_g_iss_queue.html
- list_g_loc.html
- list_g_org.html
- list_g_prod.html
- list_g_qname.html
- list_g_srvrs.html
- list_g_tblmap.html
- list_g_tblrule.html
- list_g_tenant.html
- list_help_item.html
- list_help_set.html
- list_ical_event_template.html
- list_imp.html
- list_in.html
- list_iss.html
- list_issalg.html
- list_isscat.html
- list_issstat.html
- list_iss_kt.html

- list_iss_wf.html
- list_kc.html
- list_KCAT_LINKED.html
- list_KCAT_QA.html
- list_KCAT_tree.html
- list_KD.html
- list_kdsched.html
- list_kdsched_config.html
- list_KD_ATTMNT.html
- list_kd_CI_DOC_LINKS.html
- list_KD_FILE.html
- list_kd_INDEX_DOC_LINKS.html
- list_KD_QA.html
- list_KEIT_export_transactions.html
- list_KEIT_IMPORT_PACKAGES.html
- list_KEIT_import_transactions.html
- list_KEIT_TEMPLATES.html
- list_KT_ACT_CONTENT.html
- list_KT_BLC.html
- list_KT_FILE_TYPE.html
- list_KT_FLG_TYPE.html
- list_KT_FREE_TEXT.html
- list_KT_LIFE_CYCLE_REP.html
- list_ldap.html
- list_ldap_group.html
- list_loc.html
- list_LONG_TEXTS.html
- list_lr.html
- list_macro.html
- list_macro_type.html
- list_menu_bar.html
- list_menu_tree_name.html
- list_mfrmod.html

- list_mgs.html
- list_mgsalg.html
- list_mgsstat.html
- list_NOTIFICATION.html
- list_no_contract_sdsc.html
- list_nr.html
- list_nrf.html
- list_nr_com.html
- list_ntfl.html
- list_ntfm.html
- list_ntfr.html
- list_OA_TABLES.html
- list_options.html
- list_org.html
- list_O_EVENTS.html
- list_pcat.html
- list_pcat_cr.html
- list_pcat_in.html
- list_pcat_pr.html
- list_perscnt.html
- list_position.html
- list_pr.html
- list_pri.html
- list_prod.html
- list_prod_list.html
- list_prpval.html
- list_prpval_rule.html
- list_QUERY_POLICY.html
- list_QUERY_POLICY_ACTIONS.html
- list_rc.html
- list_rel_cat.html
- list_response.html
- list_role.html

- list_role_tab.html
- list_rptmeth.html
- list_rrf.html
- list_rss.html
- list_sapolicy.html
- list_saprobtyp.html
- list_sdsc.html
- list_sdsc_map.html
- list_seq.html
- list_sev.html
- list_showgrp.html
- list_site.html
- list_srvr_aliases.html
- list_srvr_zones.html
- list_state.html
- list_svc_contract.html
- list_svy_atpl.html
- list_svy_qtpl.html
- list_svy_tpl.html
- list_tab.html
- list_tenant.html
- list_tenant_group.html
- list_tskstat.html
- list_tskty.html
- list_tspan.html
- list_typecnt.html
- list_tz.html
- list_urg.html
- list_usp_servers.html
- list_vpt.html
- list_web_form.html
- list_wf.html
- list_wrkshft.html

- load_properties.html
- load_wait.html
- loc_address_tab.html
- loc_auto_assignment_tab.html
- log_reader.html
- log_reader_banner.html
- log_reader_fs.html
- log_sol_4itil.html

M

- macro_atomic_cond_tab.html
- macro_cnt_tab.html
- macro_ctp_tab.html
- macro_ntfl_tab.html
- macro_rrf_tab.html
- mactyp_exescript_tab.html
- mactyp_valscript_tab.html
- mapped_contracts_tab.html
- menubar.template
- menubar_admin.html
- menubar_architect.html
- menubar_chg_sched.html
- menubar_dtbuilder.html
- menubar_html_editor.html
- menubar_kt.html
- menubar_no.html
- menubar_sd.html
- menubar_sd_chg_manager.html
- menubar_sd_cust_mgr.html
- menubar_sd_cust_rep.html
- menubar_sd_hd_manager.html
- menubar_sd_inc_manager.html
- menubar_sd_know_analyst.html
- menubar_sd_know_manager.html

- menubar_sd_l1_analyst.html
- menubar_sd_l2_analyst.html
- menubar_sd_prb_manager.html
- menubar_sd_vendor_analyst.html
- menu_frames.html
- menu_tree_editor.html
- menu_tree_editor2.html
- menu_tree_editor3.html
- mgs_cnt_tab.html
- mgs_ctp_tab.html
- mgs_ini_tab.html
- mgs_ntfl_tab.html
- mgs_rem_tab.html
- multiframe.template
- multiframe_reports_admin.html
- multiframe_reports_chg_manager.html
- multiframe_reports_cust_mgr.html
- multiframe_reports_inc_mgr.html
- multiframe_reports_know_analyst.html
- multiframe_reports_know_mgr.html
- multiframe_reports_prb_mgr.html
- multiframe_reports_sd_mgr.html

N

- new_lr.html
- nf.html
- nosession.html
- nr_bm_tab.html
- nr_chg_tab.html
- nr_contact_tab.html
- nr_inc_tab.html
- nr_inv_tab.html
- nr_iss_tab.html
- nr_loc_tab.html

- nr_log_tab.html
- nr_org_tab.html
- nr_prb_tab.html
- nr_projex_tab.html
- nr_rel_tab.html
- nr_reqitil_tab.html
- nr_req_tab.html
- nr_serv_tab.html
- ntfl_ntfr_tab.html
- ntfr_aty_tab.html
- ntfr_cnt_tab.html
- ntfr_ctp_tab.html
- ntfr_ntfl_tab.html

i

- order_status_change.html
- org_address_tab.html
- org_env_tab.html

P

- pcat_auto_assignment_tab.html
- pcat_prptpl_tab.html
- pcat_wftpl_tab.html
- power_user_tips.html
- profile_browser.html
- profile_browser2.html
- profile_browser3.html
- profile_browser_frameset.html
- profile_envcnt.html
- profile_envorg.html
- profile_histcnt_chg.html
- profile_histcnt_cr.html
- profile_histcnt_in.html
- profile_histcnt_iss.html

- profile_histcnt_pr.html
- profile_historg_chg.html
- profile_historg_cr.html
- profile_historg_in.html
- profile_historg_iss.html
- profile_historg_pr.html
- profile_infocnt.html
- profile_infoorg.html
- profile_menu.html
- profile_qtemplate.html
- pr_attinc_tab.html
- pr_relreq_tab.html

R

- reports.html
- reports.html.tpl
- request_status_change.html
- role_auth_tab.html
- role_fnacc_tab.html
- role_goform_tab.html
- role_kt_ct_tab.html
- role_kt_docs_tab.html
- role_webform_tab.html
- role_web_interface_tab.html

S

- sapolicy_ac_tab.html
- sapolicy_pt_tab.html
- saprobtyp_dh_tab.html
- saprobtyp_rd_tab.html
- scoreboard.html
- scratchpad.html
- screen_reader_usage.html
- sdsc_chg_slatpl_tab.html

- sdsc_chg_wf_slatpl_tab.html
- sdsc_cr_slatpl_tab.html
- sdsc_iss_slatpl_tab.html
- sdsc_iss_wf_slatpl_tab.html
- sdsc_map_cnt_tab.html
- sdsc_map_grp_tab.html
- sdsc_map_nr_tab.html
- sdsc_map_pri_tab.html
- sdsc_map_urg_tab.html
- sd_kt_admin.html
- sd_main.html
- sd_main_role.html
- search_child_KCATs_filter.html
- show_error.html
- show_main_detail.html
- std_body.html
- std_body_site.html
- std_footer.html
- std_footer_site.html
- std_head.html
- std_head_site.html
- suggest_knowledge_isscat.html
- suggest_knowledge_list_isscat.html
- suggest_knowledge_list_pcat.html
- suggest_knowledge_pcat.html
- sugggest_knowledge_search_options.html

T

- tab_detail.template
- tenant_address_tab.html
- tenant_groups_tab.html
- tenant_group_members_tab.html
- tskty_tskstat_tab.html

U

- update_lrel_bmrep.html
- update_lrel_chg.html
- update_lrel_chgcat.html
- update_lrel_cnt.html
- update_lrel_cr.html
- update_lrel_ctp.html
- update_lrel_goform.html
- update_lrel_help_content.html
- update_lrel_in.html
- update_lrel_iss.html
- update_lrel_isscat.html
- update_lrel_loc.html
- update_lrel_macro.html
- update_lrel_nr.html
- update_lrel_ntfl.html
- update_lrel_ntfr.html
- update_lrel_org.html
- update_lrel_pcat.html
- update_lrel_pr.html
- update_lrel_role.html
- update_lrel_tab.html
- update_lrel_tenant.html
- update_lrel_tenant_group.html
- update_lrel_tskstat.html
- update_lrel_webform.html
- update_lrel_wrkshft.html
- upd_chg_sched.html
- upload_file.html
- upload_success.html
- usq_update.html
- usq_update_control.html
- usq_update_fin.html

- usq_update_select.html
- usq_update_tree.html

V

- v30_date_helper.html

W

- wfdef.html
- wftpl_auto_assignment_tab.html
- wftpl_bhvtpl_tab.html
- working.html
- workitems.html
- wrkshft_auto_assignment_tab.html
- wrkshft_schedule_tab.html
- wspmain.html

X

- xfer_esc_chg.html
- xfer_esc_cr.html
- xfer_esc_iss.html
- xx_attmnt_tab.html
- xx_candp_tab.html
- xx_nr_tab.html
- xx_prop_tab.html
- xx_solnalg_tab.html
- xx_stype_tab.html
- xx_template_tab.html
- xx_wf_tab.html