

CA Enterprise Log Manager

Guía de administración

Versión 12.5.01



Esta documentación, que incluye sistemas incrustados de ayuda y materiales distribuidos por medios electrónicos (en adelante, referidos como la "Documentación") se proporciona con el único propósito de informar al usuario final, pudiendo CA proceder a su modificación o retirada en cualquier momento.

Queda prohibida la copia, transferencia, reproducción, divulgación, modificación o duplicado 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 (i) un acuerdo suscrito aparte entre Vd. y CA que rijan su uso del software de CA al que se refiere la Documentación; o (ii) 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, o procurar de alguna otra forma, un número razonable de copias de la Documentación, que serán exclusivamente para uso interno de Vd. y de sus empleados, y cuyo uso deberá guardar relación con dichos productos. En cualquier caso, en dichas copias deberán figurar los avisos e inscripciones relativas a los derechos de autor de CA.

Este derecho a realizar copias de la Documentación sólo tendrá validez durante el período en que la licencia aplicable para el software en cuestión 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, ANTE VD. NI ANTE TERCEROS, EN LOS SUPUESTOS DE DEMANDAS POR PÉRDIDAS O DAÑOS, DIRECTOS O INDIRECTOS, QUE SE DERIVEN DEL USO DE ESTA DOCUMENTACIÓN INCLUYENDO A TÍTULO ENUNCIATIVO PERO SIN LIMITARSE A ELLO, LA PÉRDIDA DE BENEFICIOS Y DE INVERSIONES, LA INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL, LA PÉRDIDA DEL FONDO DE COMERCIO O LA PÉRDIDA DE DATOS, INCLUSO CUANDO CA HUBIERA PODIDO SER ADVERTIDA CON ANTELACIÓN Y EXPRESAMENTE DE LA POSIBILIDAD DE DICHAS PÉRDIDAS O DAÑOS.

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 esta 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 © 2011 CA. Todos los derechos reservados. Todas las marcas registradas y nombres comerciales, logotipos y marcas de servicios a los que se hace referencia en este documento pertenecen a sus respectivas compañías.

Referencias a productos de CA

En este documento se hace referencia a los siguientes productos de CA:

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- Centro de comandos de seguridad de CA (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

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>.

Cambios en la documentación

Se han realizado actualizaciones en las áreas siguientes desde la última versión de esta documentación: Servicios y adaptadores de CA, consultas e informes y agentes.

Los temas afectados son los siguientes:

- Servicios y adaptadores de CA
 - Configuraciones del servicio: temas nuevos y actualizados para cubrir los cambios en las actualizaciones de lista con clave, integración con ObserveIT y las consideraciones del servidor de informes.
- Consultas e informes:
 - Formato de fecha y hora: tema nuevos para cubrir la configuración de la función de formato de fecha y hora.
 - Vista de consulta: tema actualizado acerca del cambio en la vista de la función de consulta.
 - Listas con clave: tema actualizado acerca del cambio en el proceso de valores dinámicos de IT PAM.
- Agentes:
 - Configuración del agente y del grupo de agentes: temas actualizados sobre los cambios en los procesos de agente.
 - Archivo de diagnóstico del agente: tema nuevo acerca de la nueva herramienta AgentDiagnostics.

Más información:

[Configuración de la integración de CA IT PAM](#) (en la página 160)

[Integración de ObserveIT](#) (en la página 162)

[Consideraciones del servidor de informes](#) (en la página 175)

[Formato de fecha y hora](#) (en la página 283)

[Visualización de consultas](#) (en la página 287)

[Creación de una lista con claves](#) (en la página 356)

[Configuración de un agente](#) (en la página 669)

[Adición de agentes a grupos de agentes](#) (en la página 679)

[Creación de un archivo de diagnóstico del agente para el Departamento de Soporte Técnico.](#) (en la página 691)

Contenido

Capítulo 1: Introducción 21

Acerca de esta guía	21

Capítulo 2: Cuentas de usuario 25

Tareas de administración automática	25
Desbloqueo de cuentas de usuario	26
Cambio de contraseñas	27
Tareas asociadas a funciones	27
Tareas de auditor	28
Tareas del analista	30
Tareas del administrador	31
Configuración de cuentas con la configuración predeterminada	39
Creación de grupos globales	40
Creación de un usuario global	41
Asignación de funciones a usuarios globales	42
Gestión de cuentas de usuarios relacionadas	44
Directrices de activación de usuarios	44
Edición de cuentas de usuario	45
Restablecimiento de contraseñas de usuario	48
Eliminación de cuentas de usuario	49

Capítulo 3: Políticas 51

Introducción a las políticas	52
Políticas de acceso predefinidas	52
Examen de políticas de todos los usuarios	53
Examen de políticas de auditores	57
Examen de políticas de analistas	59
Examen de políticas de administradores	62
Políticas de acceso para productos registrados	64
Copia de seguridad de todas las políticas de acceso	65
Restauración de políticas de acceso	70

Capítulo 4: Políticas y funciones personalizadas

75

Directrices para la creación de políticas	76
Tipos de políticas de acceso a CALM	80
Recursos y acciones	83
Recursos de CALM y carpetas de EEM	86
Recursos globales y funcionalidad de CA EEM	89
Planificación de la función del usuario	90
Configuración de políticas de acceso y funciones de usuario personalizadas	91
Creación de un grupo de usuarios de la aplicación (función)	95
Concesión de acceso a CA Enterprise Log Manager a funciones personalizadas	96
Adición de identidades a una política existente	98
Creación de una política de acceso a CALM	99
Creación de política de ámbito	102
Creación de una política basada en una política existente	106
Comprobación de una política nueva	108
Creación de políticas de grupos dinámicos de usuarios	109
Creación de un filtro de acceso	111
Mantenimiento de cuentas de usuario y políticas de acceso	113
Creación de un calendario	113
Adición de un calendario a una política	115
Ejemplo: Limitar el acceso a los días laborables	116
Exportación de políticas de acceso	118
Supresión de políticas personalizadas	119
Eliminación de filtros de acceso y políticas de obligación	120
Ejemplo: Permitir a un usuario que no es administrador gestionar acciones de almacenamiento ...	121
Restricción del acceso a datos a un usuario: caso de Win-Admin	125
Paso 1: Creación del usuario Win-Admin	127
Paso 2: Adición de Win-Admin a la política de acceso a la aplicación de CALM	128
Paso 3: Creación de una política de acceso al sistema de Win-Admin	129
Paso 4: Creación de un filtro de acceso a datos de Win-Admin	133
Paso 5: Inicio de sesión como usuario Win-Admin	136
Paso 6: Ampliación de las acciones permitidas	137
Restricción de acceso a una función: caso de analista de PCI	139
Paso 1: Planificación de la función y de las políticas que se desean crear	140
Paso 2: Creación de la función de analista de PCI	141
Paso 3: Adición de analistas de PCI a la política de acceso a la aplicación de CALM	142
Paso 4: Adición de analistas de PCI a políticas existentes	142

Paso 5: Creación de políticas basadas en políticas de edición y visualización de informes de analistas	143
Paso 6: Asignación de la función de analista de PCI a un usuario	144
Paso 7: Inicio de sesión como analista de PCI y evaluación del acceso	144
Políticas de ejemplo para integraciones personalizadas	146
Políticas de ejemplo para reglas de supresión y resumen	148

Capítulo 5: Servicios y adaptadores de CA **151**

Tareas de servicios	152
Eliminación de hosts de servicio	153
Edición de configuraciones globales	154
Edición de configuraciones del servicio global	157
Edición de configuraciones del servicio local	158
Configuraciones de servicio	159
Consideraciones del servicio de alertas	160
Consideraciones del servicio de correlación	167
Consideraciones del almacén de registro de eventos	168
Consideraciones del servicio del incidente	173
Consideraciones sobre el servidor ODBC	174
Consideraciones del servidor de informes	175
Consideraciones acerca del servicio de prueba de reglas	176
Consideraciones de la suscripción	177
Servicio Estado del sistema	181
Tareas de configuración de adaptadores de CA	182
Edición de configuraciones de adaptadores globales	183
Edición de configuraciones de adaptadores locales	184
Visualización de eventos autocontrolados del adaptador	185
Visualización del estado del adaptador	186
Consideraciones del servicio de SAPI	187
Consideraciones de iTechnology Event Service	189
Tareas de estado del sistema	189
Creación de un archivo de diagnóstico para soporte	190
Reinicio de un servidor host	191
Reinicio de los servicios de CA ELM	191
Revisión del estado y la versión del servicio	192
Revisión de los eventos autocontrolados de estado del sistema	192

Capítulo 6: Almacenamiento de registros 193

Acerca del almacenamiento de registros	194
Estados de la base de datos de registro de eventos	196
Copia de seguridad y restauración de ACS	199
Comprobaciones de la integridad de datos	200
Activación de comprobación de la integridad automática	200
Programación de una comprobación de la integridad de datos	201
Comprobación de la integridad de datos a petición	201
Firma de bases de datos en cuarentena	202
Alternancia de claves	202
Importación de claves	203
Exportación de claves	203
Configuración de autenticaciones no interactivas para su restauración	204
Ejemplo: configuración de la autenticación desde un servidor de almacenamiento remoto a un servidor de punto de restauración	205
Ejemplo: configuración de la autenticación de un servidor de almacenamiento a un servidor de informes	208
Consulta del catálogo de archivado	211
Restauración de archivos almacenados de forma automática	213
Script de restauración para restaurar bases de datos almacenadas	214
Copia de seguridad manual de bases de datos archivadas	217
Identificación de bases de datos que no tienen copia de seguridad	217
Realización de copias de seguridad	219
Registro de las copias de seguridad	219
Restauración manual de archivos en el sistema de almacenamiento de registro de eventos original	221
Preparación para restaurar bases de datos almacenadas	223
Desplazamiento de bases de datos archivadas a un directorio de archivo	225
Restauración de archivos almacenados de forma manual	226
Verificación de la restauración	228
Restauración manual de archivos en sistemas de almacenamiento de registro de eventos nuevos ..	228
Configuración del número máximo de días de archivado para los archivos restaurados	230
Adición de bases de datos restauradas al catálogo	231
Seguimiento de copia de seguridad/restauración de LMArchive	232

Capítulo 7: Suscripción 235

Actualización a la versión 12.5 de CA Enterprise Log Manager mediante suscripción	235
Consulta del estado de suscripción global	237

Consulte el estado de suscripción de un servidor	238
Edición de la configuración de suscripción global	240
Edición de la configuración de suscripción local de los servidores	241
Descarga y selección de módulos para la suscripción sin conexión	243
Acerca de las actualizaciones a petición	245
Inicio de actualizaciones a petición	247
Espacio libre en disco para actualizaciones	249
Acerca de las claves públicas de suscripción	250
Eventos autocontrolados para suscripción	250
Control de los eventos de suscripción	251
Visualización de detalles de eventos de suscripción	254
Aplicación de actualizaciones de suscripción a agentes y conectores	255

Capítulo 8: Filtros y perfiles **259**

Capítulo 9: Filtros globales y locales **261**

Acerca de los filtros simples	262
Establecimiento de filtros simples	263
Acerca de los filtros de perfiles	264
Creación de perfiles	265
Apertura del asistente de perfiles	266
Adición de detalles de perfiles	266
Creación de filtros de datos	267
Creación de filtros de etiquetas	268
Importación de perfiles	269
Exportación de perfiles	270
Establecimiento de perfiles	270
Creación de filtros globales	271
Configuración de los ajustes de consultas globales	273
Edición de filtros globales	274
Eliminación de filtros globales	274
Creación de filtros locales	275
Edición de filtros locales	276
Eliminación de filtros locales	276

Capítulo 10: Consultas e informes **277**

Acerca de las consultas y los informes	278

Asignación de etiquetas a tareas	281

Capítulo 11: Formato de fecha y hora **283**

Formatos de fecha y hora compatibles	284
Cambio del formato de fecha y hora	286
Visualización de consultas	287
Visualización de informes	288
Desactivación de la visualización del informe seleccionado	290
Ejemplo: Ejecutar informes de PCI	291
Visualización de la lista de informes mediante la etiqueta de PCI	291
Búsqueda de informes de un control PCI DDS específico	292
Trabajo con un único informe de PCI	295
Peticiones	296
Uso de la petición del conector	298
Utilización de la petición de host	301
Utilización de la petición de IP	303
Utilización de la petición de nombre de registro	306
Utilización de la petición de puerto	308
Utilización de la petición de usuario	310
Creación de consultas	313
Apertura del asistente de diseño de consulta	314
Adición de detalles de consultas	315
Adición de columnas de consulta	316
Configuración de filtros de consultas	319
Configuración de condiciones del resultado	324
Creación de visualizaciones de pantallas de consulta	329
Adición de informes de obtención de detalles	330
Edición de consultas	331
Eliminación de consultas personalizadas	331
Desactivación de la visualización de la consulta seleccionada	332
Exportación e importación de definiciones de consultas	332
Exportación de definiciones de consultas	333
Importación de definiciones de consultas	334
Creación de informes	335
Apertura del asistente de diseño de informe	335
Adición de detalles del informe	336
Establecimiento de diseños de informes	337
Ejemplo: Crear informes a partir de consultas existentes	338

Ejemplo: configuración de la federación y de los informes federados	341
Edición de informes	346
Eliminación de informes personalizados	346
Ejemplo: Eliminar informes diarios con más de 30 días de antigüedad	347
Exportación de definiciones de informes	348
Importación de definiciones de informes	349
Preparación para el empleo de informes mediante listas con clave	350
Activación de la importación de valores dinámicos	351
Enfoques para el mantenimiento de listas con clave	355
Creación de valores con clave para informes predefinidos	365
Visualización de un informe mediante una lista con clave	370

Capítulo 12: Alertas de acción **371**

Acerca de las alertas de acción	372
Utilización de consultas etiquetadas como alertas de acción	373
Identificación de otras consultas que se pueden utilizar para las alertas	375
Personalización de consultas para las alertas de acción	376
Identificación del filtro simple para eventos graves	377
Creación de una consulta para recuperar sólo eventos graves	379
Personalización de consultas para recuperar sólo eventos graves	381
Consideraciones de las alertas de acción	388
Trabajo con procesos de salida de alerta/evento de CA IT PAM	391
Acerca de los procesos de salida de alerta/evento de CA IT PAM	392
Importación del proceso de salida de alerta/evento de ejemplo	400
Directrices para la creación de un proceso de alerta/evento	407
Obtención de detalles para integración de CA IT PAM	411
Ejemplo: Ejecución de un proceso de salida de alerta/evento con resultados de la consulta seleccionada	415
Diseño de consultas para eventos que se envían al proceso de salida de alerta/evento	419
Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por fila	421
Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por consulta	426
Trabajo con mensajes SNMP	429
Acerca de los mensajes SNMP	429
Ejemplo: filtros simples para alertas que se enviarán como mensajes SNMP	430
Acerca de los archivos MIB	431
Proceso de trabajo con mensajes SNMP	448
Configuración de la integración con un destino de trap de SNMP	450
Preparación de CA Spectrum para recibir mensajes SNMP desde alertas	451

Ejemplo: Alerta a CA Spectrum de cambios de configuración	456
Preparación de CA NSM para que reciba mensajes SNMP desde alertas	461
Ejemplo: cómo alertar a CA NSM acerca de los cambios en la configuración	466
Creación de alertas de acción	475
Apertura del asistente de programación de alertas de acción	476
Selección de consultas de alerta	477
Establecimiento de parámetros de programación de tareas de alerta	478
Configuración de destinos de las notificaciones	479
Definición de destinos de las consultas de tareas de alerta	485
Ejemplo: Crear una alerta de acción para el espacio en disco bajo	486
Ejemplo: Crear una alerta para un evento autocontrolado	490
Ejemplo: Envío de un correo electrónico al Administrator cuando se detiene el flujo de eventos	493
Configuración de retenciones de alertas de acción	496
Ejemplo: Crear una alerta para Business_Critical_Sources	497
Edición de alertas de acciones	499
Activación o desactivación de alertas de acción	500
Eliminación de alertas de acciones	501

Capítulo 13: Informes programados 503

Visualización de informes generados	503
Filtrado de informes	504
Anotación de informes generados	505
Programación de tareas de informes	506
Apertura del asistente de programación de informes	507
Selección de plantillas de informes	508
Uso de filtros avanzados	509
Configuración de condiciones del resultado	511
Establecimiento de parámetros de programación	515
Selección de ajustes de formato y notificación	516
Selección de un objetivo de consulta de informe	517
Ejemplo: Programar informes con una etiqueta común	517
Ejemplo: Enviar por correo electrónico de forma diaria informes de PCI en formato PDF	521
Edición de tareas de informes programadas	522
Activación y desactivación de tareas de informes programados	523
Eliminación de tareas de informes programadas	524
Eventos autocontrolados	524
Visualización de eventos autocontrolados	525

Capítulo 14: Supresión y resumen 527

Versiones de componentes de refinamiento de eventos	527
Tareas de reglas de resumen y supresión	528
Efectos de las reglas de supresión	529
Creación de reglas de supresión	530
Creación de reglas de resumen	536
Aplicación de reglas de resumen o supresión	543
Aplicación de supresiones y resúmenes en componentes de agentes	543
Copia de reglas de resumen o supresión	547
Edición de reglas de resumen o supresión	548
Eliminación de reglas de resumen o supresión	549
Importación de reglas de resumen o supresión	550
Exportación de reglas de resumen o supresión	551
Creación de la regla de supresión del evento de Windows 560	552

Capítulo 15: Asignación y análisis 555

Estados de eventos	556
Tareas de reglas de asignación y análisis	558
Creación de archivos de análisis de mensajes	558
Apertura del asistente para el archivo de análisis	560
Definición de detalles de archivo	560
Carga de eventos de ejemplo	562
Adición de campos globales	563
Creación de filtros de coincidencia previa	564
Creación de filtros de análisis	566
Análisis del archivo XMP	576
Creación de archivos de asignación de datos	577
Apertura del asistente para el archivo de asignación	580
Provisión de detalles de archivos	581
Ofrecimiento de eventos de ejemplo	581
Establecimiento de asignaciones directas	583
Establecimiento de asignaciones de función	584
Establecimiento de asignaciones de función de concatenación	586
Establecimiento de asignaciones condicionales	588
Establecimiento de asignaciones de bloque	589
Realización de análisis de asignaciones	591
Tareas de reglas de transferencia de eventos	592
Creación de reglas de transferencia de eventos	592

Acerca de los eventos de syslog reenviados	599
Edición de reglas de transferencia	600
Supresión de reglas de transferencia	600
Importación de reglas de transferencia	601
Exportación de reglas de transferencia	602

Capítulo 16: Integraciones y conectores 603

Tareas de integración y conectores	603
Creación de una integración	605
Apertura del asistente de integración	606
Adición de componentes de integración	607
Aplicación de reglas de resumen y supresión	608
Establecimiento de configuraciones predeterminadas	609
Establecimiento de configuraciones del registro de archivos	610
Creación de escuchas de syslog	613
Apertura del asistente de escucha	614
Adición de componentes de escucha	615
Aplicación de reglas de resumen y supresión	616
Establecimiento de configuraciones predeterminadas	617
Adición de zonas horarias a syslog	619
Creación de versiones de integraciones nuevas	620
Eliminación de integraciones	621
Exportación e importación de definiciones de integraciones	621
Importación de definiciones de integraciones	622
Exportación de definiciones de integraciones	623
Creación de conectores	623
Apertura del asistente de conector	624
Adición de detalles de conectores	625
Aplicación de reglas de resumen y supresión	626
Establecimiento de configuraciones de conectores	626
Visualización de conectores	627
Vista de guía del conector	628
Edición de conectores	629
Acerca de las configuraciones guardadas	629
Creación de configuraciones guardadas	630
Configuración de conectores de forma masiva	631
Apertura del asistente de configuración de orígenes de recopilación	632
Selección de detalles del origen	633

Aplicación de reglas de supresión	634
Aplicación de reglas de resumen	634
Configuración del conector	635
Selección de agentes y asignación de orígenes	636
Actualización de varias configuraciones de conectores	637

Capítulo 17: Correlación de eventos y gestión de incidentes 639

Capítulo 18: Tareas de regla de correlación 641

Acerca de las reglas de correlación	642
Uso de reglas de correlación predefinidas	643
Uso de listas con claves con reglas de correlación	647
Ejemplo: Creación de un archivo CSV para realizar pruebas	648
Acerca de las notificaciones de incidentes	648
Cómo diseñar y aplicar notificaciones de incidentes	650

Capítulo 19: Tareas de gestión de incidentes 655

Consulta de detalles de incidentes	656

Capítulo 20: Agentes 657

Planificación de la instalación de agentes	657
Planificación de configuraciones de agentes	661
Planificación de recopilación directa de registros	662
Planificación de recopilación de registros sin agente	664
Planificación de recopilaciones de registros mediante agente	664
Selección del nivel que se va a configurar	665
Tareas de gestión de agentes	666
Actualización de la clave de autenticación del agente	667
Descarga de binarios del agente	668
Configuración de un agente	669
Control de archivos de configuración manipulada	672
Visualización del cuadro de mandos de los agentes	673
Visualización y control del estado de agentes o conectores	675
Creación de grupos de agentes	677
Apertura del asistente para grupos de agentes	677
Adición de detalles a grupos de agentes	678
Adición de agentes a grupos de agentes	679

Configuración de la gestión de agentes	680
Apertura del asistente de asignación de servidores del gestor de registros	681
Selección de agentes de destino	682
Selección de gestores de registros	683
Protección de los agentes contra el impacto de los cambios de dirección IP del servidor	684
Disponibilidad de servidores con direcciones IP dinámicas	685
Disponibilidad de servidores durante la reasignación de direcciones IP estáticas	685
Aplicación de actualizaciones de suscripción	687
Apertura del asistente de listas de actualizaciones	688
Selección de los agentes o conectores que se van a actualizar	689
Actualización de versiones de integración de agentes o conectores	690
Creación de un archivo de diagnóstico del agente para el Departamento de Soporte Técnico.	691

Capítulo 21: Certificados personalizados 693

Implementación de certificados personalizados	693
Adición del certificado de raíz de confianza al servidor de gestión de CA Enterprise Log Manager ...	694
Adición de certificados de raíz de confianza para todos los demás servidores de CA Enterprise Log Manager	696
Adición del nombre común del certificado a una política de acceso	697
Implementación de certificados nuevos	698

Apéndice A: Funcionalidades de accesibilidad 701

Modo de accesibilidad	701
Controles de accesibilidad	701
Configuración de idiomas en CA Enterprise Log Manager	702
Localización manual de CA Enterprise Log Manager	703

Apéndice B: Acceso a eventos recopilados con ODBC y JDBC 705

Acerca del acceso mediante ODBC/JDBC en CA Enterprise Log Manager	705
Creación de consultas relativas a ODBC y JDBC para el uso con CA Enterprise Log Manager	706
Limitaciones de soporte de SQL	706
Funciones SQL compatibles	707
Procesamiento de las consultas	708
Alias de la columna de resultado	709
Límites de resultados	709
Códigos de error específicos de CA Enterprise Log Manager	710
Ejemplo: Empleo de un filtro de acceso para limitar los resultados de ODBC	710

Ejemplo: Preparación para el uso de clientes de ODBC y JDBC con Crystal Reports	712
Creación de un usuario de CA Enterprise Log Manager para el acceso de ODBC o JDBC	713
Configuración de los ajustes de servicio ODBC	714
Creación de un origen de datos ODBC "elm"	714
Edición del archivo de configuración de Crystal Reports	717
Creación de eventos para el ejemplo de ODBC	719
Uso de Crystal Reports para acceder al almacén de registro de eventos con ODBC	720
Acceso a eventos desde Crystal Reports con JDBC	721
Copia de archivos JAR del controlador de JDBC	721
Uso de Crystal Reports para acceder al almacén de registro de eventos con JDBC	722
Supresión del cliente de ODBC en sistemas Windows	723
Supresión de clientes de JDBC	723

Glosario	725

Índice	759

Capítulo 1: Introducción

Esta sección contiene los siguientes temas:

[Acerca de esta guía](#) (en la página 21)

Acerca de esta guía

Esta *Guía de administración de CA Enterprise Log Manager* hace referencia a las tareas llevadas a cabo antes de que el administrador instale CA Enterprise Log Manager y realice la configuración inicial del servidor. Algunas de estas tareas se llevan a cabo para incluir cambios poco frecuentes en el sistema; otras son tareas de rutina realizadas de forma programada; y otras tareas son tareas de control permanente.

Esta guía está diseñada para todos los públicos, incluidos los siguientes:

- Administradores que mantienen la configuración del producto y gestionan el almacenamiento de los registros y las actualizaciones de suscripción
- Analistas que emplean los informes para controlar el entorno, crear informes personalizados y programar la generación de alertas
- Auditores que programan informes, emplean consultas e informes para verificar la conformidad con los estándares y realizan anotaciones en los informes

Esta guía incluye un glosario de términos y un índice. A continuación, se muestra un resumen del contenido:

Sección	Describe cómo
Cuentas de usuario	Configurar cuentas de usuario con funciones predefinidas y administrar automáticamente cuentas de usuario
Políticas	Planificar funciones personalizadas y políticas asociadas mediante el empleo de funciones y políticas predefinidas
Políticas y funciones personalizadas	Restringir el acceso del usuario mediante funciones personalizadas, políticas personalizadas y filtros de acceso
Servicios y adaptadores de CA	Configurar el almacén de registro de eventos, el servidor de informes, el servicio de suscripción y determinados adaptadores de eventos

Sección	Describe cómo
Almacenamiento de registros	Configurar el almacenamiento automático y restaurar bases de datos almacenadas
Suscripción	Mantener la configuración de la suscripción, aplicar actualizaciones y restaurar una copia de seguridad de suscripción
Filtros y perfiles	Limitar los datos mostrados en un informe o en una consulta, o en todos los informes y en las consultas con filtros. Limite las listas de etiquetas, consultas e informes con perfiles.
Consultas e informes	Crear, editar e importar o exportar consultas e informes para visualizar los registros de eventos recientes y actuales
Alertas de acción	Crear una alerta de acción para notificar a los usuarios o a los destinos de trap de SNMP, o para ejecutar un proceso de IT PAM cuando se producen eventos especificados
Informes programados	Programar y mantener tareas de informes; visualizar y anotar los informes generados
Supresión y resumen	Crear y emplear reglas de supresión y resumen para reducir la carga del servidor y evitar la recopilación o el procesamiento de eventos no deseados
Asignación y análisis	Crear y emplear reglas de asignación y análisis para refinar eventos sin formato de varios formatos en valores estandarizados y compatibles con la gramática de eventos comunes, así como crear reglas de transferencia de eventos
Integraciones y conectores	Crear integraciones de productos que, al implementarse como conectores, permiten refinar y transmitir eventos de un origen de eventos único al servidor de CA Enterprise Log Manager
Agentes	Planificar el empleo de agentes, preparar la instalación de agentes, configurar agentes y grupos de agentes y aplicar actualizaciones de suscripción a agentes
Certificados personalizados	Implementar certificados personalizados para sustituir los certificados predefinidos
Funciones de accesibilidad	Usar controles de accesibilidad
Acceso a eventos recopilados con ODBC/JDBC	Puede configurar informes personalizados con una utilidad de generación de informes de terceros o recuperar información de registro seleccionada con productos de terceros.

Nota: Para obtener más información acerca de la compatibilidad del sistema operativo o acerca de los requisitos del sistema, consulte las *Notas de la versión*. Para obtener un tutorial sobre la organización de un sistema único de manera que se puedan ver los resultados de las consultas en los eventos de syslog y Windows recopilados, consulte la *Guía de descripción de problemas*. Para más información acerca de los procedimientos a seguir paso a paso para la instalación de CA Enterprise Log Manager y la configuración inicial, consulte la *Guía de implementación*. Para obtener información detallada sobre la instalación de agentes, consulte la *Guía de instalación del Agente*. Para obtener ayuda acerca del uso de cualquier página de CA Enterprise Log Manager, vea la Ayuda en línea.

Capítulo 2: Cuentas de usuario

Esta sección contiene los siguientes temas:

- [Tareas de administración automática](#) (en la página 25)
- [Tareas asociadas a funciones](#) (en la página 27)
- [Configuración de cuentas con la configuración predeterminada](#) (en la página 39)
- [Creación de grupos globales](#) (en la página 40)
- [Creación de un usuario global](#) (en la página 41)
- [Asignación de funciones a usuarios globales](#) (en la página 42)
- [Gestión de cuentas de usuarios relacionadas](#) (en la página 44)
- [Directrices de activación de usuarios](#) (en la página 44)
- [Edición de cuentas de usuario](#) (en la página 45)
- [Restablecimiento de contraseñas de usuario](#) (en la página 48)
- [Eliminación de cuentas de usuario](#) (en la página 49)

Tareas de administración automática

Los usuarios con acceso a CA Enterprise Log Manager pueden cambiar sus propias contraseñas y desbloquear una cuenta de usuario bloqueada si el almacén de usuarios configurado es el predefinido, el almacén de usuarios de CA Enterprise Log Manager.

Cuando el administrador crea una nueva cuenta de usuario, se asigna una contraseña nueva. El usuario cambia dicha contraseña durante el primer inicio de sesión por una contraseña nueva que cumpla con las políticas de contraseñas que establecen si se permite una contraseña que coincida con el nombre de usuario, la longitud mínima y máxima, el número máximo de caracteres repetidos y la cantidad mínima de caracteres numéricos. El usuario es responsable de modificar las contraseñas con la frecuencia establecida en las políticas de contraseñas en cuanto a la antigüedad mínima y máxima de una contraseña.

Los usuarios individuales administran sus propias cuentas de estas maneras:

- Modifican las contraseñas de un modo adecuado según lo establecido por las políticas de contraseñas
- Desbloquean cuentas de usuario que se han bloqueado si así lo permite la política de contraseñas relacionada

Desbloqueo de cuentas de usuario

Puede desbloquear una cuenta de usuario bloqueada independientemente de su función, siempre y cuando la política de contraseñas lo permita. Cuando la cuenta se bloquee, tiene que desbloquearla otro usuario para que pueda acceder usted a los privilegios que le concede su función.

Las acciones de bloqueo y desbloqueo se controlan mediante las políticas de contraseñas siguientes:

- Bloquear la cuenta de usuario tras <n> inicios de sesión erróneos
- Permitir que los usuarios desbloqueen contraseñas

Las cuentas de usuario pueden bloquearse si la política de contraseñas se define para bloquear las cuentas de usuario tras un determinado número de inicios de sesión erróneos y el usuario inicia sesión con credenciales no válidos una cantidad de veces que supera el umbral especificado.

Cualquier usuario puede desbloquear la cuenta de otro usuario si la política de contraseñas se establece para permitir a los usuarios desbloquear contraseñas. Necesita la contraseña del usuario para desbloquear su cuenta de usuario.

Para desbloquear cuentas de usuario

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Desbloqueo de usuarios en el panel izquierdo.
3. Introduzca el nombre y la contraseña del usuario y, a continuación, haga clic en Desbloquear.

La cuenta de usuario se desbloquea.

Cambio de contraseñas

Puede cambiar su propia contraseña independientemente de su función. Si la política de contraseñas se establece para una duración máxima de las contraseñas, deberá cambiar su contraseña con la frecuencia indicada en dicha política.

Asegúrese de cambiar la contraseña lo antes posible en los casos siguientes:

- Si se la ha suministrado a alguien para desbloquear su cuenta
- Si olvidó su contraseña y el administrador se la ha restablecido

Para cambiar contraseñas

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Cambiar contraseña en el panel izquierdo.
3. Introduzca la contraseña antigua.
4. Introduzca la contraseña nueva dos veces.
5. Haga clic en Aceptar.

Tareas asociadas a funciones

Los administradores asignan funciones a usuarios según las tareas que deben llevar a cabo. Puede asignar a los usuarios las funciones predefinidas Auditor, Analyst y Administrator o las funciones personalizadas que cree. Para evaluar el impacto del empleo de las funciones predefinidas, revise las tareas asociadas a cada función.

Más información:

[Tareas de auditor](#) (en la página 28)

[Tareas del analista](#) (en la página 30)

[Tareas del administrador](#) (en la página 31)

Tareas de auditor

Los auditores internos pueden llevar a cabo tareas como las siguientes:

- Búsqueda de una consulta seleccionada y visualización de los resultados de dicha consulta
- En el caso de una fila de resultados de la consulta seleccionada, ejecución de un proceso de salida de alerta/evento configurado en CA IT PAM
- Visualización de los informes actuales
- Programación de informes
- Visualización de la lista de tareas de informes programadas
- Visualización de la lista de informes generados
- visualizar y anotar informes generados; y
- Configuración de filtros y perfiles

Al crear cuentas de usuario para el personal de terceros, puede asignar la función con privilegios bajos de Auditor. Por ejemplo, cuando una alerta programada ejecuta un proceso de salida de alerta/evento en el nivel de la consulta, la alerta envía una dirección URL a CA Enterprise Log Manager, que se añade a la descripción. Para que el personal de terceros pueda acceder a CA Enterprise Log Manager, necesita cuentas de usuario.

Nota: Los analistas y los administradores pueden llevar a cabo todas las tareas de los auditores, así como las tareas específicas de su función.

Los auditores externos que obtienen un acceso temporal a CA Enterprise Log Manager durante el período de la auditoría del sitio pueden verificar el cumplimiento de los estándares en las áreas siguientes:

- Verificación de que se han recopilado los registros de los orígenes correctos.
- Verificación de que existen los procedimientos necesarios para evitar la pérdida de datos. Por ejemplo, verificación de que se realizan copias de seguridad de los datos con la frecuencia suficiente como para no perder nada.
- Verificación de que los registros se revisan con regularidad para detectar problemas de seguridad.
- Verificación de que los registros se almacenan de forma adecuada en un archivo seguro.
- Verificación de que la antigüedad de los datos archivados cumple con los estándares de retención de registros.

- Verificación de que el contenido de los registros incluye el contenido necesario para la retención.

Más información:

[Programación de tareas de informes](#) (en la página 506)

[Visualización de informes generados](#) (en la página 503)

[Anotación de informes generados](#) (en la página 505)

[Visualización de informes](#) (en la página 288)

[Ejemplo: Ejecución de un proceso de salida de alerta/evento con resultados de la consulta seleccionada](#) (en la página 415)

[Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por consulta](#) (en la página 426)

Tareas del analista

Los analistas del sistema controlan la red de recopilación de registros y, a continuación, reúnen y distribuyen los datos de los informes.

Los administradores asignan la *función Analyst* a usuarios que son responsables de las tareas siguientes:

- Creación y edición de consultas e informes personalizados

Un informe es una pantalla gráfica o en forma de tabla de datos de registro de eventos generada mediante la ejecución de consultas predefinidas o personalizadas con filtros. Los datos pueden proceder de bases de datos calientes, tibias y descongeladas del sistema de almacenamiento de registro de eventos del servidor seleccionado y, si se solicita, de sus servidores federados.

- Programación de alertas de acción

Una alerta de acción es una tarea de consulta programada que se puede emplear para detectar infracciones de políticas, tendencias de uso, patrones de inicio de sesión y otros datos que pueden requerir atención a corto plazo. Los datos de la alerta se pueden ver en la interfaz de usuario o a través de una fuente RSS. Puede enviar una alerta programada a los destinatarios de correo electrónico, un destino de mensaje SNMP o un proceso de salida de alerta/evento de CA IT PAM. El proceso se puede realizar una vez por fila o una vez por consulta.

- Creación de etiquetas

Una *etiqueta* es una frase clave o un término empleado para identificar consultas o informes pertenecientes a la misma categoría. Para agregar un informe nuevo a una tarea programada configurada para seleccionar informes con una etiqueta específica, agregue la etiqueta común al informe nuevo. Una etiqueta también puede ser una frase clave asociada a una consulta que, por lo tanto, describe el contenido de la consulta y permite realizar una búsqueda y una clasificación basadas en la frase clave.

- Visualización de fuentes RSS

Un *evento RSS* (del inglés Rich Site Summary) es un evento generado por CA Enterprise Log Manager para transmitir una alerta de acción a usuarios y productos de terceros. El evento consta de un resumen del resultado de cada alerta de acción, así como de un vínculo al archivo de resultados. Se puede configurar la duración de un determinado elemento de fuente RSS.

Los analistas pueden emplear el siguiente sistema a medida que se familiaricen con el empleo de CA Enterprise Log Manager:

1. Examinar los informes predefinidos disponibles. (Los auditores también pueden hacerlo.)
2. También se pueden diseñar informes personalizados, crear etiquetas para dichos informes, así como planificar, visualizar y anotarlos.
3. Programar informes de interés para la generación regular. (Los auditores también pueden hacerlo.)
4. Revisar informes generados e introducir anotaciones. (Los auditores también pueden hacerlo.)
5. Identificar criterios para el envío de una alerta, el formato que se debe emplear y el destinatario. A continuación, programar la alerta para generarla cuando se cumplan los criterios.

Tareas del administrador

Los usuarios a los que se asigna la función Administrator tienen acceso ilimitado a las funciones disponibles en todas las fichas de CA Enterprise Log Manager. Sólo aquellos usuarios a los que se haya asignado la función Administrator tienen acceso ilimitado a la ficha Administración. En la ficha Administración, los administradores configuran y mantienen todos los aspectos de la recopilación de datos, todos los servicios y todos los accesos de usuario.

Más información:

[Configuración y personalización de la recopilación de registros](#) (en la página 32)

[Configuración y control de los servicios](#) (en la página 34)

[Gestión de usuarios y accesos](#) (en la página 37)

Configuración y personalización de la recopilación de registros

Sólo aquellos usuarios con la función Administrator pueden configurar y mantener funciones relacionadas con la recopilación de registros. Los administradores realizan tareas de recopilación de registros en la subficha Recopilación de registros de la ficha Administración.

Utilizan el Explorador de recopilación de registros para configurar conectores en los agentes, algo que es necesario para la recopilación de registros. También aplican actualizaciones de suscripción a los agentes, si procede.

El empleo de la biblioteca de refinamiento de eventos es opcional. La funcionalidad predeterminada, que se actualiza con regularidad, está diseñada para satisfacer las necesidades de la mayoría de los clientes.

Entre las tareas de los administradores que implican la recopilación de registros se incluyen las siguientes:

- Configure y gestione los agentes instalados desde un servidor de CA Enterprise Log Manager dedicado a la recopilación.
- Envíe una consulta al catálogo de archivos en un servidor de informes de CA Enterprise Log Manager.

El *catálogo de archivos* es el registro de todas las bases de datos que han figurado alguna vez en el servidor de CA Enterprise Log Manager. Esto incluye las bases de datos creadas recientemente, las que cuentan con copia de seguridad y se han trasladado y las que se han suprimido antes de realizar la copia de seguridad, si las hubiera.

- Configure los adaptadores de CA empleados por CA Audit.
- Gestione la biblioteca de refinamiento de eventos.
 - Trabaje con integraciones predefinidas y cree nuevas integraciones desde el principio o basadas en una copia de una integración predefinida.

La integración es el método a través del cual se procesan los eventos no clasificados para convertirlos en eventos refinados, de manera que se puedan visualizar en consultas e informes.

- Cree una escucha de syslog a partir de la escucha predefinida.
- Cree nuevos archivos de análisis desde el principio o basados en una copia de un archivo predefinido seleccionado.

Un archivo de análisis de mensajes (XMP), asociado con un tipo de origen de evento específico, aplica reglas de análisis que descomponen el evento sin formato en pares de nombre/valor.

- Cree nuevos archivos de asignación desde el principio o basados en una copia de un archivo predefinido seleccionado.

Los archivos de asignación de datos (DM) son archivos XML que emplean la gramática de eventos comunes (CEG) de CA para transformar eventos del formato de origen a un formato que se pueda almacenar para generación de informes y análisis en el almacén de registro de eventos.

- Cree reglas de resumen desde el principio o basadas en una copia de una regla predefinida seleccionado.

Las reglas de resumen son reglas que combinan determinados eventos nativos del mismo tipo en un evento refinado.

- Cree reglas de supresión desde el principio o basadas en una copia de una regla predefinida seleccionado.

Las reglas de supresión evitan que aparezcan determinados eventos refinados en los informes.

- Cree reglas de transferencia de eventos.

Las reglas de transferencia de eventos especifican los eventos seleccionados que se transferirán a los productos de terceros, como aquellos que correlacionan eventos después de haberlos guardado en el almacén de registro de eventos.

- Cree perfiles.

Un perfil especifica el conjunto de filtros de datos y etiquetas que se pueden seleccionar. Los filtros de datos limitan los datos que se muestran en la consulta o el informe; los filtros de etiquetas limitan las etiquetas que se muestran en la lista de etiquetas de consulta y en la lista de etiquetas de informe.

Más información:

[Creación de grupos de agentes](#) (en la página 677)

[Configuración de la gestión de agentes](#) (en la página 680)

[Aplicación de actualizaciones de suscripción](#) (en la página 687)

Configuración y control de los servicios

Sólo aquellos usuarios con el rol de administrador pueden configurar y mantener los servicios a los que se puede acceder desde la subficha Servicios de la ficha Administración. Configure todos los servicios después de instalar CA Enterprise Log Manager.

Entre las tareas de los administradores que implican servicios se incluyen las siguientes:

- Configuración de servicios globales, como los siguientes:
 - Intervalo de actualización
 - Tiempo de espera de sesión
 - Si se necesita autenticación para ver las alertas publicadas en las fuentes RSS
 - Etiquetas que se deben ocultar
 - Perfil predeterminado
- Configuración del servicio de almacén de registro de eventos.
 - En el nivel global, configure servicios que se apliquen a todos los servidores de CA Enterprise Log Manager.
 - En el nivel local, configure autoarchivado.

El sistema de almacenamiento de registro de eventos del servidor de recopilación de CA Enterprise Log Manager alberga una base de datos caliente de registros nuevos. La base de datos caliente se comprime en forma de base de datos tibia cuando alcanza el número máximo de filas.

- Si se ha configurado el archivado automático entre el servidor de recopilación y el servidor de informes, la base de datos tibia se copiará en el servidor de informes y, a continuación, se suprimirá del servidor de recopilación.
- Si configura el archivado automático entre el servidor de informes y un servidor remoto que no sea un servidor de CA Enterprise Log Manager, las bases de datos tibias se copian en el servidor remoto cada día o cada hora, en función de la configuración actual del archivado automático. De forma predeterminada, el servidor de informes conserva las bases de datos hasta llegar a los límites establecidos de tiempo o espacio en disco. Las bases de datos se suprimen automáticamente del servidor de informes solamente si se selecciona la casilla de verificación Servidor de ELM remoto.

- Si no se ha configurado el archivado automático del servidor de informes a un servidor de almacenamiento remoto, deberá crear de forma manual una copia de seguridad de las bases de datos tibias y desplazarlas al sistema de almacenamiento a largo plazo. La base de datos tibia se guarda en el sistema de almacenamiento de registro de eventos de un servidor de informes (o servidor de gestión/informes en una implementación de dos servidores) durante la cantidad de días configurada como número máximo de días de almacenamiento, a no ser que el espacio disponible caiga por debajo del porcentaje configurado de espacio en disco para archivo. En este caso, las bases de datos tibias se eliminan, comenzando por la más antigua.
- Configuración del servicio del servidor de informes.

El servicio del servidor de informes gestiona informes y alertas, incluidas políticas de retención, el formato de los informes que se imprimen o se envían por correo electrónico y los valores con clave de los informes y las alertas. Además, gestiona la configuración de integración de los procesos de CA IT PAM como, por ejemplo, salida de alerta/evento y valores dinámicos para destinos y alertas de mensajes SNMP.
- Configuración de actualizaciones de suscripción.

Las actualizaciones de suscripción hacen referencia a los archivos binarios y no binarios que ofrece el servidor de suscripciones de CA a los servidores de CA Enterprise Log Manager, el componente CA EEM del servidor de gestión y los agentes.
- Gestión de la federación de servidores de CA Enterprise Log Manager.

En el servidor de gestión, puede establecer una consulta para incluir en la federación a secundarios y equivalentes. Los servidores de CA Enterprise Log Manager se pueden federar con dos objetivos:

 - El servidor de recopilación archiva de forma automática cada base de datos caliente en forma de base de datos tibia y la envía al servidor de informes relacionado. Cree una federación entre el servidor de recopilación y el servidor de informes. Cuando envía una consulta al servidor de gestión con la federación seleccionada, puede obtener resultados no sólo de las bases de datos tibias locales, sino también de la base de datos caliente del servidor de recopilación.

- Pueden crearse múltiples servidores de informes para distribuir el almacenamiento de bases de datos tibias entre múltiples sistemas de almacenamiento de registro de eventos. Los servidores de informes se pueden federar en combinación con cada servidor de recopilación federado como secundario del servidor de informes correspondiente. Las consultas federadas de cualquiera de los servidores de informes combinados dan como resultado datos tanto de los servidores combinados (equivalentes) como de todos sus servidores secundarios.

Nota: Si crea un CA Enterprise Log Manager de punto de restauración con la intención de restaurar las bases de datos archivadas de almacenamiento a largo plazo, es conveniente dejar ese servidor fuera de la federación.

- Control y gestión del estado del sistema.

Más información:

[Copia de seguridad y restauración de ACS](#) (en la página 199)

[Consulta del catálogo de archivado](#) (en la página 211)

[Restauración de archivos almacenados de forma automática](#) (en la página 213)

[Script de restauración para restaurar bases de datos almacenadas](#) (en la página 214)

[Consideraciones sobre el servidor ODBC](#) (en la página 174)

[Creación de un archivo de diagnóstico para soporte](#) (en la página 190)

[Reinicio de un servidor host](#) (en la página 191)

[Reinicio de los servicios de CA ELM](#) (en la página 191)

[Revisión del estado y la versión del servicio](#) (en la página 192)

[Revisión de los eventos autocontrolados de estado del sistema](#) (en la página 192)

Gestión de usuarios y accesos

Sólo los usuarios con la función Administrator pueden configurar y mantener cuentas de usuario, políticas y otros objetos de aplicación a los que se puede acceder desde la subficha Gestión de usuario y accesos de la ficha Administración. Para iniciar sesión en CA Enterprise Log Manager, los usuarios deben tener una cuenta de usuario configurada con una función y credenciales para iniciar sesión. Las funciones y las políticas predefinidas permiten que los administradores configuren acceso de usuario mediante la definición de cuentas de usuario. La creación de funciones y políticas personalizadas es opcional.

Entre las tareas de los administradores que implican a los usuarios y el acceso se incluyen las siguientes:

- Definición de usuarios globales nuevos (si el almacén de usuarios es el valor predeterminado, el almacén de usuarios de CA Enterprise Log Manager).

Al agregar un usuario nuevo, crea un usuario global. Los detalles como el nombre, la ubicación y el número de teléfono se consideran globales porque se pueden compartir. Un *usuario global* es la información de cuenta de usuario que excluye los detalles específicos de la aplicación.

- Recuperación de usuarios relacionados (si el almacén de usuarios es un almacén de usuarios relacionados).

Los detalles de usuarios globales se guardan en el almacén de usuarios configurado, que puede ser un directorio externo.

- Asigne grupos de aplicaciones (funciones) predefinidos o personalizados a usuarios nuevos o relacionados.

Los detalles de la aplicación siempre se almacenan en el repositorio del servidor de gestión. Estos son los detalles cargados en formato de sólo lectura cuando se configura un almacén de usuarios externo.

- Edite, elimine y visualice cuentas de usuario.
- Creación de grupos de aplicaciones (funciones) personalizados y políticas asociadas.

La creación de funciones comienza por la definición de un nuevo grupo de usuarios de la aplicación y, a continuación, por la creación de una política que defina las acciones permitidas en los recursos especificados. Una función del usuario puede ser un grupo de usuarios de la aplicación predeterminado o un grupo de aplicaciones definido por el usuario. Es necesario contar con funciones de usuarios personalizadas cuando los grupos de la aplicación predeterminados (Administrator, Analyst y Auditor) no están lo suficientemente depurados como para reflejar las asignaciones de trabajo. Las funciones de usuarios personalizadas requieren el empleo de políticas de acceso personalizado y la modificación de las políticas predefinidas para incluir la función nueva.

- Edición, supresión y visualización de grupos de aplicaciones y políticas asociadas.
- Edición de la política de acceso a la aplicación de CALM.

La política de acceso a la aplicación de CALM es un tipo de lista de control de acceso de política de ámbito que define quién puede acceder a CA Enterprise Log Manager. De forma predeterminada, el administrador [del grupo], el analista [del grupo] y el auditor [del grupo] pueden acceder.

- Creación, edición, supresión y visualización de las políticas de acceso.

Una política de acceso es una regla que otorga o deniega a una identidad (usuario o grupo de usuarios) los derechos de acceso a un recurso de la aplicación.

- Configuración, edición, supresión y visualización de filtros de acceso.

Un filtro de acceso es un filtro que el administrador puede emplear para controlar qué datos de eventos pueden visualizar los grupos o los usuarios que no son administradores. Por ejemplo, un filtro de acceso puede restringir los datos que pueden ver en un informe las identidades especificadas. Los filtros de acceso se convierten de forma automática en políticas de obligación.

Más información:

[Creación de grupos globales](#) (en la página 40)
[Creación de un usuario global](#) (en la página 41)
[Asignación de funciones a usuarios globales](#) (en la página 42)
[Copia de seguridad de todas las políticas de acceso](#) (en la página 65)
[Restauración de políticas de acceso](#) (en la página 70)
[Configuración de políticas de acceso y funciones de usuario personalizadas](#) (en la página 91)
[Adición de identidades a una política existente](#) (en la página 98)
[Creación de una política de acceso a CALM](#) (en la página 99)
[Creación de políticas de grupos dinámicos de usuarios](#) (en la página 109)
[Creación de una política basada en una política existente](#) (en la página 106)
[Creación de política de ámbito](#) (en la página 102)
[Creación de un filtro de acceso](#) (en la página 111)
[Creación de un grupo de usuarios de la aplicación \(función\)](#) (en la página 95)
[Concesión de acceso a CA Enterprise Log Manager a funciones personalizadas](#) (en la página 96)
[Comprobación de una política nueva](#) (en la página 108)
[Creación de un calendario](#) (en la página 113)

Configuración de cuentas con la configuración predeterminada

Si configura un entorno de prueba temporal, puede establecer la gestión de usuarios y accesos con mucha rapidez si utiliza la configuración predeterminada de las cuentas de usuario y configura sólo los campos obligatorios. Para realizar la configuración mínima con los ajustes predeterminados, cree cuentas de usuario para usuarios de CA Enterprise Log Manager del modo siguiente:

- Si utiliza el almacén de usuarios predeterminado, cree una cuenta con el nombre del usuario, asigne un grupo de aplicaciones predefinido (Administrator, Analyst o Auditor) y asigne una contraseña temporal.
- Si se trata de un almacén de usuarios externo, busque al usuario global por su nombre, asigne una función predefinida (Administrator, Analyst o Auditor) y asigne una contraseña temporal.

Más información:

[Creación de un usuario global](#) (en la página 41)
[Asignación de funciones a usuarios globales](#) (en la página 42)
[Gestión de cuentas de usuarios relacionadas](#) (en la página 44)

Creación de grupos globales

La capacidad de crear grupos globales depende de la configuración del almacén de usuarios. Tenga en cuenta lo siguiente:

- Si emplea un almacén de usuarios predeterminado, la creación de grupos globales es una tarea opcional.
- Si se trata de un almacén de usuarios externo, los grupos globales y las cuentas de usuario se cargan automáticamente en el almacén de usuarios predeterminado. También puede crear políticas personalizadas para estos grupos globales, pero no puede crear grupos globales nuevos.
- Si el almacén de usuarios en cuestión es CA SiteMinder, puede emplear grupos globales tal y como se definen en este producto de CA o puede crear nuevos grupos globales a partir de pertenencias a grupos existentes.

Para crear grupos globales

1. Haga clic en la ficha Administración y, a continuación, en la subficha Gestión de usuarios y accesos.
2. Haga clic en Grupos en el panel de la izquierda.
Aparecen los paneles de búsqueda de grupos y de grupos de usuarios.
3. Haga clic en el botón de nuevo grupo global situado junto a la carpeta de grupos globales.
Aparece el panel de creación de un nuevo grupo global de usuarios.
4. Introduzca un nombre y, de forma opcional, una descripción.
5. Si este grupo global debe contener otros grupos globales, lleve a cabo lo siguiente:
 - a. Introduzca los criterios de búsqueda para mostrar un grupo y haga clic en Buscar.
 - b. Desplace el grupo que desee incluir en la lista de grupos globales de usuarios seleccionados.
 - c. Repita esta acción hasta que la lista contenga todos los grupos que desea seleccionar.
6. Haga clic en Guardar.
Aparece un cuadro de diálogo de confirmación.

Más información:

[Planificación de la función del usuario](#) (en la página 90)

Creación de un usuario global

Sólo puede crear usuarios nuevos si el almacén de usuarios está configurado como almacén de usuarios de CA Enterprise Log Manager, que es el predeterminado. Sólo los administradores pueden crear cuentas de usuario nuevas.

Si se trata de un almacén de usuarios externo, las cuentas de usuario se cargan automáticamente en el almacén de usuarios predeterminado como registros de sólo lectura. Si necesita crear un usuario nuevo, debe hacerlo en el almacén de usuarios externo. El registro nuevo se carga de forma automática.

Para emplear el producto de CA Enterprise Log Manager, el usuario debe tener una cuenta de usuario global. Dicha cuenta debe estar activa en el momento del inicio de sesión. Las cuentas pueden desactivarse si las suspende el administrador, pueden bloquearse debido a la infracción de una política de contraseñas o pueden desactivarse porque haya transcurrido el tiempo de activación de la cuenta.

Para crear una cuenta de usuario global nueva

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en el botón Usuarios.
3. Compruebe que la cuenta que desea crear no existe. Seleccione Usuarios globales y haga clic en Ir. Si el nombre no aparece en los resultados, continúe.
4. Haga clic en el botón Nuevo usuario situado a la izquierda del árbol de usuarios.
Aparece la página Nuevo usuario.
5. Introduzca el nombre del usuario en el campo de entrada Nombre.
6. (Opcional) Asigne un grupo de usuarios de la aplicación.
 - a. Haga clic en Agregar detalles del usuario de la aplicación.
 - b. Seleccione uno o varios grupos de usuarios disponibles y haga clic en el botón de movimiento para desplazar la selección al cuadro de grupos de usuarios seleccionados.
Nota: Si no lo hace en este momento, puede editar la cuenta de un usuario global más adelante para asignar un grupo de usuarios de la aplicación.
7. Introduzca la información general de los detalles de usuarios globales.

8. (Opcional) Asigne un grupo global de usuarios.
9. Introduzca la información de autenticación:
 - a. Para establecer un umbral referente al número de inicios de sesión incorrectos que se aceptarán antes de bloquear la cuenta, introduzca un número en el campo de recuento de inicios de sesión incorrectos. Si configura el recuento con el valor 0, no se establecerá ningún límite.
 - b. Acepte la cancelación de la casilla de anulación de la política de contraseñas a no ser que desee permitir que este usuario disponga de contraseñas que no cumplan con la política de contraseñas.
 - c. Repita la contraseña introducida en el cuadro Confirmar contraseña.
 - d. Seleccione la opción de cambio de contraseña en el siguiente inicio de sesión para permitir que el usuario cambie la contraseña.
 - e. No seleccione la opción de suspensión al crear una cuenta nueva.
 - f. Introduzca una contraseña nueva en Nueva contraseña y seleccione Confirmar contraseña.
 - g. Si este usuario sólo debe tener un acceso temporal, introduzca un intervalo de fechas para activar y desactivar la cuenta de usuario.
 - h. Para aplazar la activación de la cuenta de usuario a una fecha posterior, introduzca la fecha de activación de la cuenta.
10. Haga clic en Guardar.
11. Haga clic en Cerrar.

Asignación de funciones a usuarios globales

Puede buscar una cuenta de usuario existente y asignar el grupo de usuarios de la aplicación de la función que desee que lleve a cabo el usuario. Si emplea un almacén de usuarios externo, la búsqueda da como resultado registros globales cargados desde dicho almacén de usuarios. Si el almacén de usuarios configurado es el de CA Enterprise Log Manager, la búsqueda obtiene registros creados para usuarios en CA Enterprise Log Manager.

Los administradores son los únicos que pueden editar cuentas de usuario.

Para asignar una función o un grupo de usuarios de la aplicación a un usuario existente

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.

2. Haga clic en Usuarios en el panel de la izquierda.

Aparecen los paneles Buscar usuarios y Usuarios.

3. Seleccione Usuarios globales, introduzca los criterios de búsqueda y haga clic en Ir.

Si la búsqueda es de cuentas de usuario cargadas, el panel Usuarios muestra la ruta y las etiquetas de la ruta indican el directorio externo al que se hace referencia.

Importante: Introduzca siempre criterios al realizar una búsqueda para evitar que aparezcan todas las entradas de un almacén de usuarios externo.

4. Seleccione un usuario global que no pertenezca al grupo de aplicaciones de CA Enterprise Log Manager.

La página Usuario muestra, con el nombre de carpeta, los detalles de usuarios globales y, si procede, la pertenencia a grupos globales.

5. Haga clic en Agregar detalles del usuario de la aplicación.

El panel de detalles del usuario de "CAELM" se expande.

6. Seleccione el grupo deseado en los grupos de usuarios disponibles y haga clic en la flecha hacia la derecha.

El grupo seleccionado aparece en el cuadro de grupos de usuarios seleccionados.

7. Haga clic en Guardar.

8. Verifique la adición.

- a. En el panel Buscar usuarios, haga clic en Detalles del usuario de la aplicación y haga clic en Ir.

- b. Verifique que el nombre del nuevo usuario de la aplicación aparece en los resultados que se muestran.

9. Haga clic en Cerrar.

Gestión de cuentas de usuarios relacionadas

Puede emplear información de cuentas de usuarios globales cuando hace referencia a un almacén de usuarios externo. Aunque no pueda actualizar el registro de usuarios en el almacén de usuarios externo desde CA Enterprise Log Manager, puede asignar detalles en el ámbito de la aplicación.

Tenga en cuenta los métodos siguientes para gestionar el acceso de los usuarios con cuentas guardadas en un almacén de usuarios externos.

- Agregue una función o un grupo de usuarios de la aplicación predefinido a la cuenta de usuario.
- Agregue el grupo global a las políticas predefinidas que ofrecen el acceso deseado al usuario en cuestión.
- Cree funciones personalizadas y políticas asociadas y agregue la función personalizada a la cuenta de usuario.

Directrices de activación de usuarios

Tenga en cuenta las directrices siguientes a la hora de emplear las funciones de activación de cuentas:

- Cuando cree un determinado número de cuentas de usuario a la vez, puede emplear la fecha de activación para especificar una fecha futura en la que se activarán todas las cuentas o las seleccionadas. Esto le permite ordenar por etapas el inicio de los derechos de acceso para coordinarlo con posibles formaciones que desee ofrecer a los usuarios nuevos.
- Al crear cuentas temporales para auditores externos, puede emplear los ajustes de fecha de activación y fecha de desactivación para especificar un intervalo de tiempo determinado.
- Si detecta un comportamiento sospechoso por parte de algún usuario, puede marcar de forma inmediata la cuenta correspondiente como suspendida y, de este modo, evitar que ese usuario pueda iniciar sesión de forma correcta en los servidores de CA Enterprise Log Manager.
- Cuando un usuario abandona la empresa, puede eliminar todo el registro de dicho usuario, marcarlo como suspendido o introducir una fecha de caducidad para que pase al estado de desactivación.

Más información:

[Creación de un usuario global](#) (en la página 41)

[Edición de cuentas de usuario](#) (en la página 45)

[Eliminación de cuentas de usuario](#) (en la página 49)

Edición de cuentas de usuario

Sólo los administradores pueden crear y editar cuentas de usuario. Puede buscar un usuario y mostrar la información de cuenta del usuario seleccionado por cualquiera de las razones siguientes:

- Para asignar una función de CA Enterprise Log Manager, es decir, la pertenencia a un grupo de aplicaciones, a un usuario global cuya información de cuenta se ha cargado desde un almacén de usuarios relacionados
- Para actualizar los detalles de un usuario global para una cuenta en el almacén de usuarios local
- Para suspender la cuenta de usuario
- Para restablecer la contraseña de la cuenta de un usuario porque éste olvidó la contraseña o porque la cuenta está bloqueada y la política de contraseñas no permite que los usuarios desbloqueen las cuentas de usuarios
- Para desactivar una cuenta de usuario o restablecer la duración de la cuenta activada

Importante: No introduzca datos en el campo de recuento de inicios de sesión incorrectos del área de autenticación. El sistema actualiza el valor mostrado en este campo.

Para editar cuentas de usuario

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Usuarios en el panel de la izquierda.
Aparece el panel Buscar usuarios.

3. Especifique los criterios de búsqueda en el panel Buscar usuarios a través de uno de los métodos siguientes:

- Para agregar detalles de la aplicación a un usuario global, seleccione Usuarios globales, introduzca los criterios de búsqueda y haga clic en Ir.
- Para editar la cuenta de un usuario con una función de CA Enterprise Log Manager existente, seleccione Detalles del usuario de la aplicación, introduzca los criterios de búsqueda y haga clic en Ir.

Nota: Para los criterios de búsqueda, utilice el operador LIKE cuando especifique un carácter comodín como valor, y utilice el operador EQUAL cuando especifique la cadena completa. A continuación, se muestran ejemplos:

- Pertenencia a grupo LIKE Aud*
- Pertenencia a grupo EQUALS Auditor

Los nombres de los usuarios que cumplen los criterios de búsqueda aparecen en el panel Usuarios.

4. Haga clic en el nombre de usuario de la cuenta que desee editar.
La cuenta seleccionada aparece en el panel derecho.
5. Para agregar una función, haga clic en Agregar detalles del usuario de la aplicación, seleccione la función adecuada en los grupos de usuarios disponibles y trasládelas a los grupos de usuarios seleccionados.
6. Para actualizar los detalles de un usuario global, sustituya los detalles existentes por los detalles nuevos en la sección de detalles de usuarios globales.

Nota: Sólo puede actualizar detalles mediante el almacén de usuarios predeterminado.

7. Para actualizar la configuración de autenticación, lleve a cabo una de las acciones siguientes:
 - Seleccione la anulación de la política de contraseñas para excluir a este usuario de las comprobaciones realizadas por todas las políticas de contraseñas.
 - Seleccione la suspensión para evitar que este usuario inicie sesión en cualquier servidor de CA Enterprise Log Manager.
 - Cancele la suspensión para activar esta cuenta y para que el usuario pueda iniciar sesión.
 - Si la política de contraseñas está definida para no permitir a los usuarios desbloquear contraseñas y este usuario tiene una contraseña bloqueada, seleccione Restablecer contraseña, introduzca dos veces la contraseña nueva y seleccione la opción de cambio de contraseña en el siguiente inicio de sesión.

Nota: El campo de recuento de inicios de sesión incorrectos aumenta de forma automática con cada inicio de sesión erróneo y permanece con el valor 0 si el inicio de sesión es correcto. La cuenta de un usuario se bloquea si el valor incrementado alcanza o supera el conjunto de valores de la política de contraseñas correspondiente al bloqueo de cuentas de usuarios tras una determinada cantidad de inicios de sesión erróneos.
 - Establezca una duración para el momento en el que se desea activar la cuenta. Para ello, haga clic en la fecha de activación y establezca una fecha de inicio; a continuación, haga clic en la fecha de desactivación y establezca una fecha de finalización. Los usuarios tienen acceso desde el inicio del día de la fecha de inicio hasta el final del día de la fecha de finalización. Para permitir acceso para un día, especifique la misma fecha de inicio y de finalización.
8. Haga clic en Guardar.

Las actualizaciones de la cuenta de usuario se guardan y se aplican.

Restablecimiento de contraseñas de usuario

Puede restablecer las contraseñas de usuarios que hayan olvidado su contraseña. Si un usuario queda bloqueado tras superar la cantidad configurada de intentos de inicio de sesión erróneos debido a que ha olvidado su contraseña, puede restablecerla y, a continuación, el usuario puede desbloquear la cuenta, siempre y cuando la política de contraseñas correspondiente lo permita.

Para cambiar contraseñas de usuario

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en el botón Usuarios.
3. Busque la cuenta de usuario que desea editar.
 - a. Seleccione los detalles del usuario de la aplicación.
 - b. Introduzca el nombre de usuario en el campo Valor, donde el atributo se define como Nombre de usuario y el operador se define como LIKE.
 - c. Haga clic en Ir.
4. Haga clic en el nombre de usuario en el árbol Usuarios.

Se muestran los detalles de la cuenta de usuario seleccionada.
5. En el panel Autenticación, seleccione Restablecer contraseña.

Aparecen los campos Nueva contraseña y Confirmar contraseña.
6. Introduzca la contraseña nueva en los campos Nueva contraseña y Confirmar contraseña.
7. Haga clic en Guardar y, a continuación, en Cerrar.

Eliminación de cuentas de usuario

Puede eliminar cualquier cuenta de usuario global creada en CA Enterprise Log Manager.

Puede desactivar una cuenta de usuario sin eliminarla mediante uno de los métodos siguientes:

- Puede establecer una fecha de desactivación para desactivar una cuenta en la fecha especificada.
- Puede suspender una cuenta de manera que el usuario asociado no pueda acceder a la interfaz de CA Enterprise Log Manager.

Para eliminar usuarios globales

1. Haga clic en la ficha Administración, en la subficha Gestión de usuarios y accesos y en el botón Usuarios.

Aparecen los paneles Buscar usuarios y Usuarios.

2. Seleccione Usuarios globales o Detalles del usuario de la aplicación, especifique los criterios de búsqueda y haga clic en Ir.
3. Seleccione el usuario que desea eliminar en la lista de usuarios existentes.

El registro del usuario seleccionado aparece en el panel derecho.

4. Haga clic en Suprimir.

Aparece una solicitud de confirmación para eliminar a este usuario.

5. Haga clic en Aceptar.

Aparece un mensaje que indica que el usuario global se ha eliminado correctamente.

Nota: Si vuelve a hacer clic en Ir en el panel de búsqueda de usuarios, la lista mostrada no contendrá el nombre del usuario seleccionado.

Capítulo 3: Políticas

La creación de funciones personalizadas requiere la edición de políticas predefinidas y la creación de políticas personalizadas. Antes de comenzar estas tareas, es conveniente examinar las políticas predefinidas asociadas a cada una de las funciones predefinidas. Es recomendable realizar una copia de seguridad de las políticas de acceso predefinidas antes de realizar ediciones.

Esta sección contiene los siguientes temas:

[Introducción a las políticas](#) (en la página 52)

[Políticas de acceso predefinidas](#) (en la página 52)

[Copia de seguridad de todas las políticas de acceso](#) (en la página 65)

[Restauración de políticas de acceso](#) (en la página 70)

Introducción a las políticas

Una *política de acceso* es una regla que otorga o deniega a una identidad (usuario o grupo de usuarios) los derechos de acceso a recursos de la aplicación o a recursos globales. CA Enterprise Log Manager determina si las políticas se aplican a un usuario determinado comparando identidades, recursos, clases de recursos, así como evaluando los filtros. Es decir, que una política establece las acciones que se permiten o no a identidades específicas en determinados recursos. Las políticas que no permiten el acceso a un recurso determinado tienen prioridad con respecto a las políticas que conceden el acceso a dicho recurso.

CA Enterprise Log Manager admite los siguientes tipos de políticas de acceso:

- Políticas de acceso a CALM
- Políticas de delegación
- Políticas de grupos dinámicos de usuarios (alternativa a los grupos de la aplicación personalizados)
- Políticas de obligación (creadas automáticamente cuando se crean filtros de acceso)
- Políticas de ámbito

CA Enterprise Log Manager se instala con políticas de ámbito y políticas de acceso a CALM predeterminadas para tres grupos de usuario de la aplicación de CA Enterprise Log Manager: Administrator, Analyst y Auditor. Estas políticas son suficientes si sólo pretende asignar los grupos de usuarios de la aplicación predeterminados a usuarios que realicen estas funciones.

Importante: Se recomienda que realice una copia de seguridad de las políticas predefinidas que se proporcionan con CA Enterprise Log Manager. Si una política de acceso de CALM se suprime de forma accidental, los usuarios no podrán acceder a CA Enterprise Log Manager hasta que no se restaure esa política a partir de la copia de seguridad.

Políticas de acceso predefinidas

Si sólo emplea funciones predeterminadas, en las que asigna un grupo de aplicaciones predefinido (Administrator, Analyst o Auditor) como la función para cada usuario, no es necesario que cree políticas de acceso. Todas las políticas necesarias están predefinidas y listas para usar.

Más información:

[Examen de políticas de todos los usuarios](#) (en la página 53)

[Examen de políticas de auditores](#) (en la página 57)

[Examen de políticas de analistas](#) (en la página 59)

[Examen de políticas de administradores](#) (en la página 62)

[Recursos y acciones](#) (en la página 83)

Examen de políticas de todos los usuarios

Puede examinar políticas de todos los usuarios. Edite la política de acceso a la aplicación de CALM para definir funciones personalizadas. Todas las funciones personalizadas deben añadirse como identidades a esta política.

Para examinar políticas de todos los usuarios

1. Haga clic en la ficha Administración y, a continuación, en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso en el panel izquierdo.
3. Visualice la política de acceso a la aplicación de CALM del modo siguiente:
 - a. Seleccione la opción de visualización de las políticas con nombre coincidente.
 - b. Escriba CALM*.
 - c. Haga clic en Ir.
4. Examine la política de acceso a la aplicación de CALM.

Esta política concede acceso de lectura y escritura a los recursos listados para todos los miembros de los grupos de usuarios de la aplicación predeterminados (Administrator, Analyst y Auditor) y para otros que empleen el API de CA Enterprise Log Manager:

Directivas de acceso					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	 Concesión explícita	ug:Administrator ug:Analyst ug:Auditor CALM_API_UT	read write	ApplicationInstance AppObject Policy User GlobalUser

Los recursos incluidos son los siguientes:

- El recurso Instancia aplicación es CAELM, que hace referencia al producto de CA Enterprise Log Manager.
- Política hace referencia a las políticas de acceso.
- Usuario es cualquier usuario agregado a un grupo de usuarios de la aplicación de CA Enterprise Log Manager
- Usuario global es cualquier usuario definido en el almacén de usuarios de CA Enterprise Log Manager o indicado en CA Enterprise Log Manager.
- Objeto aplicación con el valor pozFolder para la carpeta de perfiles hace referencia a los perfiles.
- AppObject con el valor pozFolder para la carpeta flex hace referencia al XML de rango de tiempo dinámico que se utiliza para rellenar la lista desplegable de rangos de tiempo en el paso Condiciones de resultados de los asistentes basados en consultas.

El filtro de acceso a la aplicación de CALM especifica los límites de acción en cada recurso.

Filtros			
WHERE	(req:resource	== val:ApplicationInstance	
Y	req:action	{}	val:read)
O	(req:resource	== val:Policy	
Y	req:action	{}	val:read)
O	(req:resource	== val:User	
Y	req:action	{}	val:read,write
Y	name:cn	== req:identity	)
O	(req:resource	== val:GlobalUser	
Y	req:action	{}	val:read
Y	name:cn	== req:identity	)
O	(req:resource	== val:AppObject	
Y	req:action	== val:read	
Y	name:pozFolder	*--* val:/CALM_Configuration/Content/Profiles	)
O	(req:action	== val:read	
Y	req:resource	== val:AppObject	
Y	name:pozFolder	*--* val:/CALM_Configuration/flex	)

5. Busque políticas para todos los usuarios del modo siguiente:
 - a. Haga clic en Políticas de acceso en el panel izquierdo.
 - b. Seleccione la opción de visualización de las políticas con identidad coincidente. Cancele la selección de otras opciones.
 - c. Introduzca [Todas las identidades] en el campo Agregar identidad.
 - d. Haga clic en Agregar.
 - e. Haga clic en Ir.

Aparecen cuatro políticas, incluidas la política de la gramática de eventos comunes y la política de acceso a datos predeterminada. (Si no introduce explícitamente [Todas las identidades], aparecerán muchas más políticas.)

6. Examine la política de acceso a datos predeterminada.

La política de acceso a datos predeterminada del tipo de recurso de CALM concede a todos los usuarios acceso a los datos de CA Enterprise Log Manager hasta los límites especificados en un filtro de acceso. Los filtros de acceso se convierten en políticas de obligación mediante la acción FulfillOnGrant en dataaccess/CALM/Data.

Directivas de acceso - "CALM"					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
Default Data Access Policy All users have access to all the data, the obligation is that access is restricted by the AccessScope	CALM	 Concesión explícita	[Todas las identidades]	dataaccess	Data

7. Examine la política de ámbito, la política de la gramática de eventos comunes.

La política de la gramática de eventos comunes predefinida permite a los usuarios con acceso a la aplicación de CALM visualizar los campos de la gramática de eventos comunes. De este modo, los campos de la gramática de eventos comunes aparecen en listas desplegables en filtros simples y avanzados para todos los usuarios, ya que todos los usuarios pueden definir filtros globales y locales para las consultas que ejecutan. Los usuarios con derecho a crear y editar consultas pueden establecer filtros para las consultas que crean y editan. Esta política también permite que todos los usuarios puedan visualizar los ajustes de la configuración global.

Directivas de acceso					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
CEG Policy All users of the CAELM have read only access on the CEG Fields. All users have read only access to the CAELM Global Configuration	SafeObject	 Concesión explícita	[Todas las identidades]	read	AppObject
Filtros					
WHERE (name:pozFolder == val:/CALM_Configuration/Content/CEG) OR (name:pozFolder *-- val:/CALM_Configuration)					

Examen de políticas de auditores

Puede examinar las políticas predefinidas de los auditores para ver cómo limitan el acceso a la aplicación a los recursos necesarios para llevar a cabo las tareas siguientes.

- Programación y anotación de informes
- Visualización de informes

Para examinar políticas predefinidas de auditores

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso en el panel izquierdo.
3. Busque políticas para auditores del modo siguiente:
 - a. Seleccione la opción de visualización de las políticas con identidad coincidente.
 - b. Introduzca ug:Auditor en el campo Agregar identidad.
 - c. Haga clic en Agregar.
 - d. Haga clic en Ir.

Aparecerán todas las políticas de [Todas las identidades] y ug:Auditor.

4. Examine la política de derechos de anotación y programación de auditores.

Todas las políticas de acceso a CALM definen las acciones que se pueden llevar a cabo con respecto a recursos específicos de la aplicación. Esta política concede a los usuarios asignados al grupo de usuarios de la aplicación, Auditor, la capacidad de programar y anotar informes.

Directivas de acceso - "CALM"					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
Auditor Schedule-Annotate Rights Auditors can schedule and Annotate reports	CALM	 Concesión explícita	ug:Auditor	schedule annotate	Report

Compare esta política con la política de creación, programación y anotación de analistas y la política de creación de administradores.

- Examine la política de acceso al servidor de informes de auditores y analistas.

Esta política de ámbito ofrece a los auditores la posibilidad de establecer el destino de los informes en cualquier servidor de informes, así como la capacidad para crear un informe federado, que solicita acceso a un sistema de almacenamiento de registro de eventos. El recurso listado en la política es Objeto aplicación; los objetos de la aplicación son los servidores de informes y los sistemas de almacenamiento de registro de eventos.

Directivas de acceso					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
Analyst Auditor Report Server Access Policy Analyst, Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	 Concesión explícita	ug:Analyst ug:Auditor	read	AppObject

Filtros

WHERE { name:pozFolder *--* val:CALM_Configuration/Modules/calmReporter }
OR { name:pozFolder *--* val:CALM_Configuration/Modules/logDepot }

Nota: Para una determinada política de acceso a CALM, es decir, una política para el tipo de recurso de CALM, suele haber una política de ámbito relacionada para la clase de recurso Objeto seguro.

- Examine la política de visualización de informes de auditores.

Esta política de ámbito ofrece a los usuarios un acceso de lectura a los informes. El recurso que se muestra en la política es Objeto aplicación.

Directivas de ámbito					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
Auditor View Report Policy Auditor can view all the Reports	SafeObject	 Concesión explícita	ug:Auditor	read	AppObject

El recurso Objeto aplicación está limitado a un recurso específico de la aplicación con un filtro que permite visualizar informes. La ruta es la ruta de una carpeta de EEM que almacena el contenido de todos los informes.

Filtros

WHERE { name:pozFolder *--* val:/CALM_Configuration/Content/Reports }

Examen de políticas de analistas

Puede examinar las políticas predefinidas de los analistas para ver cómo limitan el acceso a la aplicación a los recursos necesarios para llevar a cabo las tareas siguientes.

- Programación y anotación de informes (tareas de auditores)
- Visualización de informes (tarea de auditores)
- Creación de informes y etiquetas
- Creación y programación de alertas (consultas)
- Edición de informes, alertas y etiquetas

Para examinar políticas predefinidas de analistas

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso en el panel izquierdo.
3. Busque políticas para analistas del modo siguiente:
 - a. Borre la marca de verificación de la opción de visualización de las políticas con nombre coincidente.
 - b. Seleccione la opción de visualización de las políticas con identidad coincidente.
 - c. Introduzca ug:Analyst en el campo Agregar identidad.
 - d. Haga clic en Agregar.
 - e. Haga clic en Ir.
4. Aparecerán todas las políticas de ug:Analyst, incluidas las de [Todas las identidades], entre las que se incluye este grupo de usuarios.

5. Examine la política de creación, programación y anotación de analistas.

Esta política de acceso a CALM define las acciones que se pueden llevar a cabo con respecto a recursos específicos de la aplicación. Concede a los usuarios asignados al grupo de usuarios de la aplicación de CA Enterprise Log Manager, Analyst, la capacidad de crear, programar y anotar informes, crear y programar alertas de acción y crear etiquetas. (Los Auditors sólo pueden programar y comentar informes.)

Directivas de acceso					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	 Concesión explícita	ug:Analyst	create schedule annotate	Report Alert Tag Profile

6. Examine la política de acceso al servidor de informes de auditores y analistas.

Esta política de ámbito concede a los analistas derechos de programación en todos los servidores de informes. El recurso que se muestra en la política es Objeto aplicación.

Directivas de acceso					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	 Concesión explícita	ug:Analyst ug:Auditor	read	AppObject

Objeto aplicación está limitado a recursos específicos mediante filtros.

Filtros	
WHERE	(name:pozFolder *--* val:CALM_Configuration/Modules/calmReporter)
OR	(name:pozFolder *--* val:CALM_Configuration/Modules/logDepot)

- El filtro que termina en calmReporter concede acceso a todos los servidores de informes. Cuando se programa un informes, se especifican los servidores de informes de destino desde los que se puede visualizar el informe generado.
- El filtro que termina en logDepot concede acceso a todos los sistemas de almacenamiento de registro de eventos. Cuando un informe se define como federado, las consultas se ejecutan en los datos de todos los almacenes de registro de eventos idóneos. La idoneidad depende de la posición en la jerarquía del servidor en el que se inicia el informe en las federaciones jerárquicas.

7. Examine la política de edición y visualización de informes de analistas.

Esta política de ámbito otorga a los usuarios asignados a la función Analyst la capacidad de visualizar, editar o eliminar cualquier informe. El recurso que se especifica en la política es Objeto aplicación.

Directivas de ámbito					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identidades	Acciones	Recursos
Analyst Report View-Edit Policy Analyst can View/Edit any Report	SafeObject	 Concesión explícita	ug:Analyst	read write	AppObject

Objeto aplicación está limitado a informes mediante el filtro siguiente, que permite visualizar los informes generados almacenados en la carpeta de EEM /CALM_Configuration/Content/Reports.

Filtros
WHERE (name:pozFolder *--* val:/CALM_Configuration/Content/Reports)

Nota: La capacidad de editar informes que ofrece esta política se amplía mediante la política de la gramática de eventos comunes, que permite agregar filtros a informes mediante columnas de gramática de eventos comunes.

Examen de políticas de administradores

Los administradores asignan la función Administrator a los usuarios que tienen un acceso completo a la aplicación de CA Enterprise Log Manager y a todas sus funciones. Puede examinar las políticas predefinidas de los administradores para ver cómo otorgar acceso a los usuarios que deben llevar a cabo las tareas siguientes:

- Creación de EventGrouping, es decir, creación de reglas de supresión y resumen mediante la gramática de eventos comunes
- Creación de Integration, es decir, creación de archivos de asignación de datos y de análisis de mensajes mediante la gramática de eventos comunes
- Creación de EventForwarding, es decir, creación de reglas para la transferencia de eventos a los sistemas de terceros.
- Ejecución de Database, es decir, realización de una consulta mediante Consulta de catálogo de archivos sobre los nombres de las bases de datos que tienen copias de seguridad y se han trasladado a un sistema de almacenamiento externo
- Visualización o edición de políticas
- Visualización o edición de calendarios definidos por el usuario
- Visualización o edición de objetos de aplicación Los objetos de aplicación son plantillas de informes, plantillas de consulta, tareas de informes programados, tareas de alerta, perfiles, configuraciones de servicios, archivos de asignación de datos (DM), archivos de análisis de mensajes (XMP), reglas de supresión y resumen y reglas de transferencia de eventos.
- Creación de filtros con el atributo iPoz de AppObject
- Visualización de las carpetas incluidas en Administración, Gestión de usuarios y accesos, Carpetas de EEM y edición de los datos definidos por el usuario en esas carpetas
- Visualización o edición de detalles de usuarios de la aplicación, grupos de usuarios de la aplicación o usuarios globales
- Todas las tareas de Analyst o Auditor.

Para examinar políticas predefinidas de administradores

1. Haga clic en la ficha Administración y, a continuación, en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso en el panel izquierdo.

3. Busque políticas para administradores del modo siguiente:
 - a. Seleccione la opción de visualización de las políticas con identidad coincidente.
 - b. Introduzca ug:Administrator en el campo Agregar identidad.
 - c. Haga clic en Agregar.
 - d. Haga clic en Ir.

Aparecerán todas las políticas de [Todas las identidades] y ug:Administrator.

4. Examine la política de acceso a CALM: política de creación de administradores.

Esta política define las acciones que se pueden llevar a cabo con respecto a recursos específicos de la aplicación. Permite a los usuarios asignados al grupo de usuarios de la aplicación, Administrator, la capacidad de llevar a cabo las acciones mencionadas que se aplican a los recursos especificados.

Directivas de acceso					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
Administrator Create policy Administrator can create any object	CALM	 Concesión explícita	ug:Administrator	create schedule annotate edit	Report Alert Profile Tag Integration EventGrouping EventForwarding Database

5. Examine la política de acceso a CALM: política de gestión de agentes de administración.

Esta política concede a los administradores el derecho para crear grupos de agentes, editar todos los grupos de agentes, configurar conectores y crear integraciones. Permite a los administradores editar la clave de autenticación del agente para la instancia de la aplicación del servidor de CA Enterprise Log Manager al que el agente transfiere los eventos recopilados. De forma predeterminada, la clave de autenticación del agente se aplica a todos los servidores de CA Enterprise Log Manager de las instancias de la aplicación, pero se puede definir para que sea exclusivo para una instancia de la aplicación.

Directivas de acceso					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
Admin Agent Manager Policy Access Rights for Administrator for Agent Management	CALM	 Concesión explícita	ug:Administrator	edit	AgentConfiguration AgentAuthenticationKey Connector ALL_GROUPS Integration

6. Examine la política de ámbito: política predeterminada del administrador.

Esta política permite a los administradores visualizar, editar o eliminar los recursos listados. Los recursos incluidos no son específicos para CA Enterprise Log Manager y AppObject. AppObject se refiere los objetos específicos de la aplicación, que son los recursos incluidos en la política de creación de administradores de CALM y de gestión de agentes de administración de CALM.

Directivas de ámbito					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
Administrator Default Policy Administrators can view/modify/delete any Object	SafeObject	 Concesión explícita	ug:Administrator	read write	Policy Calendar AppObject iPoz Folder User UserGroup GlobalUserGroup GlobalUser

Políticas de acceso para productos registrados

Cuando un producto se registra mediante CA Enterprise Log Manager, se genera un certificado nuevo y se actualizan algunas políticas de acceso para permitir un acceso de sólo lectura a todas las etiquetas, consultas e informes. En concreto, el nombre de certificado empleado para autenticar el producto registrado se añade como nombre de certificado de la identidad a las políticas siguientes:

- Política de acceso a la aplicación de CALM
- Política de acceso al servidor de informes de auditores y analistas
- Política de edición y visualización de informes de analistas.

La adición del nombre de certificado a las políticas permite a los usuarios de cualquier producto de CA o de terceros, así como a clientes de CA obtener una lista de consultas e informes por etiqueta. Estos usuarios pueden visualizar las listas en su propia interfaz de usuario, así como recuperar los datos de eventos refinados que necesiten.

Copia de seguridad de todas las políticas de acceso

La exportación de políticas de acceso predefinidas es un método recomendado para guardar una copia de seguridad en el caso de que una política de acceso se elimine o se dañe de forma inadvertida.

Importante: Como las políticas pueden dañarse durante un reinicio del servicio CA EEM o del sistema, es importante contar con una copia de seguridad actualizada para realizar la restauración. Además, es conveniente realizar una copia de seguridad de CA EEM de forma periódica, por ejemplo, tras la instalación de un CA Enterprise Log Manager nuevo y después de crear políticas personalizadas.

Puede exportar todas las políticas de cada tipo de política de acceso. Al exportar políticas, se genera un archivo XML para cada política del tipo seleccionado. Los archivos XML se comprimen en un archivo denominado CAELM[1].xml.gz que contiene el documento CAELM[1].xml. Guarde el archivo comprimido exportado en el directorio que desee.

Antes de que pueda restaurar el archivo de copia de seguridad guardado, deberá copiarlo en el directorio siguiente de CA Enterprise Log Manager con el almacén de usuarios interno: /opt/CA/LogManager/EEM. Puede realizar esta copia tras realizar un almacenamiento en el directorio local o esperar y realizar la copia sólo si es necesario llevar a cabo una restauración.

El formato en el que se exportan las políticas depende del número de objetos exportados.

- *filename.tar.gz* se emplea si la cantidad de objetos exportados es grande
- *filename.xml.gz* se emplea si la cantidad de objetos exportados es pequeña o mediana

Cuando realice la exportación, es conveniente cambiarle el nombre a *filename* (CAELM[n]) por un nombre descriptivo para usted. Por ejemplo, puede exportar los archivos de las tres carpetas de políticas que contienen políticas predefinidas como CAELM_PolíticasAccesoCALM, CAELM_PolíticasEventos y CAELM_PolíticasÁmbito.

Nota: Deben mantenerse las mismas extensiones: xml.gz o tar.gz.

Puede extraer del archivo comprimido el archivo XML que contiene la definición de las políticas de acceso y emplearlo como entrada para la utilidad safex utilizada para restaurar la política de acceso.

Para realizar una copia de seguridad de todas las políticas de acceso

1. Haga clic en la ficha Administración y, a continuación, en la subficha Gestión de usuarios y accesos.
2. Realice una copia de seguridad de las políticas de acceso a CALM predefinidas del modo siguiente:

- a. Haga clic en el botón Políticas de acceso.
- b. Haga clic en CALM.

Aparece la tabla de políticas correspondiente a las políticas de acceso a CALM.

- c. Haga clic en el botón Exportar.
- d. Aparece el cuadro de diálogo de descarga de archivos con opciones de apertura y almacenamiento.
- e. (Opcional) Haga clic en Abrir para abrir el archivo comprimido CAELM[1].xml.gz. Haga doble clic en CAELM[1].xml para examinar el archivo en formato XML.
- f. Haga clic en Guardar para guardar el archivo.

Aparece el cuadro de diálogo Guardar como.

- g. Seleccione la carpeta de destino donde desea guardar el archivo, cambie el nombre del archivo si lo desea y haga clic en Guardar.

Si no cambia el nombre del archivo, el archivo comprimido se guardará como CAELM[1].xml.gz.

- h. Haga clic en Cerrar.

El cuadro de diálogo de descarga finalizada se cierra. La lista de políticas permanece visible en el panel izquierdo.

3. Realice una copia de seguridad de las políticas de evento predefinidas del modo siguiente:
 - a. Haga clic en Políticas de eventos.
Aparece la tabla de políticas correspondiente a las políticas de eventos.
 - b. Haga clic en el botón Exportar.
 - c. Aparece el cuadro de diálogo de descarga de archivos con opciones de apertura y almacenamiento.
 - d. Haga clic en Guardar para guardar el archivo.
Aparece un mensaje en el que se le pregunta si desea reemplazar el archivo CAELM[1].xml.gz existente.
 - e. Haga clic en No.
 - f. Introduzca un nombre exclusivo en el campo de nombre del archivo y haga clic en Guardar. Por ejemplo, edite la entrada como CAELM[2].xml.gz o introduzca un nombre para el tipo de política, como CAELM_PolíticasEventos.
 - g. Haga clic en Cerrar.
El cuadro de diálogo de descarga finalizada se cierra. La lista de políticas permanece visible en el panel izquierdo.

4. Realice una copia de seguridad de las políticas de ámbito predefinidas del modo siguiente:
 - a. Haga clic en Políticas de ámbito.
Aparece la tabla de políticas correspondiente a las políticas de ámbito.
 - b. Haga clic en el botón Exportar. Es posible que deba desplazarse horizontalmente para ver el botón en la esquina superior derecha.
 - c. Aparece el cuadro de diálogo de descarga de archivos con opciones de apertura y almacenamiento.
 - d. Haga clic en Guardar para guardar el archivo.
Aparece un mensaje en el que se le pregunta si desea reemplazar el archivo CAELM[1].xml.gz existente.
 - e. Haga clic en No.
 - f. Introduzca un nombre exclusivo en el campo de nombre del archivo y haga clic en Guardar. Por ejemplo, edite la entrada como CAELM[3].xml.gz o introduzca un nombre para el tipo de política, como CAELM_PolíticasÁmbito.
 - g. Haga clic en Cerrar.
El cuadro de diálogo de descarga finalizada se cierra. La lista de políticas permanece visible en el panel izquierdo.
5. Haga clic en Cerrar.
La lista de políticas de acceso se cierra.

Ejemplo: CAELM[1].xml para políticas de acceso a CALM

A continuación, se muestra la entrada de una política del archivo CAELM[1].xml.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <Safex>
  <Attach label="CAELM" />
  <Add />
- <AddOrModify>
  - <Policy folder="/" name="Auditor Schedule-Annotate Rights">
    <Description>Auditors can schedule and Annotate reports</Description>
    <ResourceClassName>CALM</ResourceClassName>
    <PolicyType>policy</PolicyType>
    <Disabled>False</Disabled>
    <ExplicitDeny>False</ExplicitDeny>
    <PreDeployment>False</PreDeployment>
    <RegexCompare>False</RegexCompare>
    <Resource>Report</Resource>
    <Action>schedule</Action>
    <Action>annotate</Action>
    <Identity>ug:Auditor</Identity>
    <Attribute name="CreateTimestamp">20080926053329</Attribute>
  </Policy>
```

Restauración de políticas de acceso

Puede restaurar una política de acceso que se haya suprimido o modificado de un modo que cause problemas. Si se suprime o se daña una política de acceso de forma accidental, los usuarios identificados como identidades en dicha política no podrán acceder a CA Enterprise Log Manager hasta que esa política se vuelva a definir o se restaure.

La restauración de políticas de acceso requiere la ejecución de la utilidad safex para políticas.

Emplee uno de los procedimientos siguientes, en función de si la exportación ha generado un archivo de copia de seguridad con la extensión xml.gz o con la extensión tar.gz.

Para restaurar políticas de acceso de una copia de seguridad denominada filename.xml.gz

1. Copie los archivos de copia de seguridad almacenados en el directorio siguiente del CA Enterprise Log Manager de gestión, que normalmente es el primer servidor instalado.

`/opt/CA/LogManager/EEM`

2. Ejecute el comando siguiente para recuperar el archivo XML:

`gunzip filename.xml.gz`

Esto da como resultado *filename.xml*.

3. (Opcional) Si sólo desea restaurar una de las políticas en el grupo del que ha realizado la copia de seguridad, lleve a cabo lo siguiente:

- a. Abra el archivo XML.
- b. En las políticas que no desee restaurar, elimine las líneas XML que comienzan y acaban por las etiquetas siguientes:
`<Policy folder="/" name=policyname>` y `</Policy>`

- c. Guarde el archivo.

4. Ejecute el comando siguiente, donde *eemserverhostname* hace referencia al nombre del host del CA Enterprise Log Manager de gestión.

`./safex -h eemserverhostname -u EiamAdmin -p password -f filename.xml`

Cuando el servidor de CA Enterprise Log Manager se encuentra en modo FIPS, asegúrese de se incluye la opción `-fips`.

La política o las políticas definidas en *filename.xml* restauradas se agregarán al tipo de política adecuado y se activarán.

Para restaurar políticas de acceso de una copia de seguridad denominada *filename.tar.gz*

1. Copie los archivos de copia de seguridad almacenados en el directorio siguiente del CA Enterprise Log Manager de gestión, que normalmente es el primer servidor instalado.

`/opt/CA/LogManager/EEM`

2. Ejecute el comando siguiente para recuperar el archivo XML:

`gunzip filename.tar.gz`

Esto da como resultado *filename.tar*.

3. Ejecute el siguiente comando:

`tar -xvf filename.tar`

Esto da como resultado *filename.xml*.

4. (Opcional) Si sólo desea restaurar una de las políticas en el grupo del que ha realizado la copia de seguridad, lleve a cabo lo siguiente:

- a. Abra el archivo XML.
- b. En las políticas que no desee restaurar, elimine las líneas XML que comienzan y acaban por las etiquetas siguientes:
`<Policy folder="/" name=polycynname>` y `</Policy>`
- c. Guarde el archivo.

5. Ejecute el comando siguiente, donde *eemserverhostname* hace referencia al nombre del host del CA Enterprise Log Manager de gestión.

`./safex -h eemserverhostname -u EiamAdmin -p password -f filename.xml`

Para volver a crear la política de acceso a CALM si no tiene copia de seguridad

Si no tiene copia de seguridad, puede volver a crear la política de acceso a la aplicación de CALM.

1. Vuelva a crear la política de acceso a la aplicación de CALM. Consulte la sección de políticas predefinidas.
2. Defina los filtros tal y como se indica en la ilustración siguiente. Las rutas parciales son las siguientes:
 - /CALM_Configuration/Content/Profiles
 - /CALM_Configuration/flex

Filtros					
Lógica	(	Valor/tipo izquierdo	Operador	Valor/tipo derecho	)
NINGUNO	(	solicitud resource	STRING EQUAL ==	valor ApplicationInstance	)
Y		solicitud action	STRING WITHINSET {}	valor read	)
O	(	solicitud resource	STRING EQUAL ==	valor Policy	)
Y		solicitud action	STRING WITHINSET {}	valor read	)
O	(	solicitud resource	STRING EQUAL ==	valor User	)
Y		solicitud action	STRING WITHINSET {}	valor read,write	)
Y		atributo con nombre cn	STRING EQUAL ==	solicitud identity	)
O	(	solicitud resource	STRING EQUAL ==	valor GlobalUser	)
Y		solicitud action	STRING WITHINSET {}	valor read	)
Y		atributo con nombre cn	STRING EQUAL ==	solicitud identity	)
O	(	solicitud resource	STRING EQUAL ==	valor AppObject	)
Y		solicitud action	STRING EQUAL ==	valor read	)
Y		atributo con nombre pozFolder	STRING CONTAINS *..*	valor /CALM_Configuration/C	)

La presencia de esta política permite que cualquier administrador inicie sesión y cree las demás políticas.

Capítulo 4: Políticas y funciones personalizadas

Esta sección contiene los siguientes temas:

[Directrices para la creación de políticas](#) (en la página 76)

[Planificación de la función del usuario](#) (en la página 90)

[Configuración de políticas de acceso y funciones de usuario personalizadas](#) (en la página 91)

[Mantenimiento de cuentas de usuario y políticas de acceso](#) (en la página 113)

[Ejemplo: Permitir a un usuario que no es administrador gestionar acciones de almacenamiento](#) (en la página 121)

[Restricción del acceso a datos a un usuario: caso de Win-Admin](#) (en la página 125)

[Restricción de acceso a una función: caso de analista de PCI](#) (en la página 139)

[Políticas de ejemplo para integraciones personalizadas](#) (en la página 146)

[Políticas de ejemplo para reglas de supresión y resumen](#) (en la página 148)

Directrices para la creación de políticas

Todas las políticas de ámbito y las políticas de acceso de CALM definen las acciones que se permiten o se deniegan a determinadas identidades en recursos específicos. Las políticas del tipo de recurso de CALM conceden o deniegan a determinadas identidades la capacidad de llevar a cabo acciones específicas de los productos en los recursos de la aplicación, también llamados recursos de CALM. Las políticas de AppObject del recurso SafeObject conceden o deniegan a determinadas identidades la posibilidad de llevar a cabo acciones de escritura o lectura en un recurso de la aplicación, tal y como se indica en los filtros. Otras políticas del tipo de recurso SafeObject conceden o deniegan a determinadas identidades la posibilidad de llevar a cabo acciones de escritura o lectura en los recursos globales.

El tipo de política o políticas que cree dependerá del recurso al que desee limitar el acceso. A continuación, se indica un resumen de los requisitos de las políticas por recurso:

- Recursos que requieren una política de CALM y políticas de ámbito para Objeto aplicación
 - Transferencia de eventos
 - EventGroupings
 - Integration (sin agente)
 - Perfil
 - Report
- Recursos que sólo requieren una política de CALM
 - AgentAuthenticationKey
 - AgentConfiguration
 - Alert
 - ALL_GROUPS
 - Connector
 - Database
 - Integration (relacionada con agentes)
 - Tag

- Recursos que sólo requieren políticas de ámbito para el recurso global
 - Calendario
 - Carpeta
 - Usuario global
 - Grupo de usuarios globales
 - iPoz
 - Política
 - Usuario
 - Grupo de usuarios

Las directrices siguientes indican las diferencias de métodos de creación de políticas. Dichas diferencias se basan en los recursos que desea controlar.

Para controlar el acceso a EventForwarding, EventGrouping, Integration, Profile y Report

El método siguiente sólo hace referencia a las políticas de los recursos de CALM EventGrouping, Integration, Profile y Report. Estos recursos de la aplicación requieren una política de CALM y dos políticas de ámbito.

1. Cree una política de CALM para uno o más recursos de la aplicación, como Report o Integration. Especifique una o más acciones específicas de la aplicación que sean válidas para los recursos especificados, como crear, programar, o anotar. Agregue las identidades a las que desee conceder o denegar las acciones.
2. Cree una política de ámbito acompañante en el recurso Objeto aplicación con acciones de lectura y escritura. Especifique la acción de escritura para permitir que la identidad edite o elimine el recurso, pero que no lo pueda crear. Especifique la acción de lectura para permitir a la identidad mostrar o visualizar el recurso. Cree un filtro que vincule el recurso Objeto aplicación al recurso de la aplicación relacionado. Especifique en el filtro la ruta de la carpeta de EEM que almacena el contenido del recurso especificado o que es un módulo para el que se requiere acceso para el recurso de la aplicación relacionado. Agregue a esta política las mismas identidades que las añadidas a la política de CALM relacionada.
3. Cree una segunda política de ámbito acompañante en el recurso AppObject que sólo posea la acción de lectura. Especifique la acción de lectura para permitir a la identidad mostrar o visualizar el recurso. Cree un filtro que vincule el recurso Objeto aplicación al recurso de la aplicación relacionado. Especifique en el filtro la ruta de la carpeta de EEM que almacena el contenido del recurso especificado o que es un módulo para el que se requiere acceso para el recurso de la aplicación relacionado. Agregue a esta política usuarios con menos privilegios o grupos de usuarios como identidades.

Para controlar el acceso a alertas, bases de datos, etiquetas y recursos relacionados con agentes

El método siguiente hace referencia a recursos de la aplicación que sólo requieren una política de CALM que conceda o deniegue el acceso.

- Cree una política de acceso a CALM para un recurso como, por ejemplo, Conector o Etiqueta. Especifique la acción de edición para permitir que la identidad cree, edite y elimine el recurso y que lleve a cabo cualquier otra acción válida. Agregue las identidades a las que desee conceder o denegar esta acción.

Nota: El acceso a recursos relacionados con agentes activa los botones de la carpeta Explorador de agentes o de sus subcarpetas en la subficha Recopilación de registros de la ficha Administración. El acceso al recurso Alert permite que la identidad acceda a la ficha Alertas. El acceso al recurso Etiqueta permite que la identidad cree una etiqueta para una consulta o un informe personalizado. El acceso al recurso Base de datos permite que la identidad ejecute una consulta de archivo.

Para controlar el acceso a los recursos globales empleados en la aplicación de CAELM

El método siguiente hace referencia a los recursos globales, que sólo requieren una política de ámbito para limitar el acceso.

1. Cree una política de ámbito para uno o más recursos globales, como Usuario o Política. Especifique la acción de escritura para permitir que la identidad cree, edite o elimine el recurso. Agregue las identidades a las que desee conceder o denegar esta acción.
2. Cree una política de ámbito para uno o más recursos globales, como Usuario o Política. Especifique la acción de lectura para permitir a la identidad visualizar el recurso global. Agregue las identidades a las que desee conceder o denegar esta acción.

Nota: Los recursos globales son los que están disponibles mediante los botones de la subficha Gestión de usuarios y accesos de la ficha Administración.

Más información:

[Tipos de políticas de acceso a CALM](#) (en la página 80)

[Recursos y acciones](#) (en la página 83)

[Recursos de CALM y carpetas de EEM](#) (en la página 86)

[Recursos globales y funcionalidad de CA EEM](#) (en la página 89)

[Creación de una política de acceso a CALM](#) (en la página 99)

Tipos de políticas de acceso a CALM

Al crear una política de acceso para CALM o una política de ámbito, seleccione uno de los tres tipos siguientes:

- Política de acceso
- Lista de control de acceso
- Lista de control de acceso de identidades

Esta selección influye en el nivel de detalle para la configuración de la política de acceso; la política de acceso es el nivel más amplio.

Nota: Los ejemplos que se muestran aquí son políticas de acceso para el tipo de recurso de CALM y, por lo tanto, incluyen acciones y recursos específicos de CA Enterprise Log Manager.

Una política de acceso especifica acciones válidas para cualquiera de los recursos seleccionados que se otorgan a todas las identidades seleccionadas. Al generar una política genérica para CA Enterprise Log Manager, añada recursos pertenecientes al tipo de recurso de CALM y, a continuación, seleccione acciones en la lista mostrada. Las acciones seleccionadas se aplican a los recursos seleccionados para los que son válidas. En este ejemplo, la política permite que las acciones seleccionadas se lleven a cabo en todos los recursos seleccionados para los que sea válida la acción de crear.

Configuración de directivas de acceso	
Recursos	Acciones
	create
	schedule
	annotate
	dataaccess
	edit
	[Todas las acciones]
Agregar recurso:   	
Alert Database EventGrouping Integration Profile Report Tag AgentConfiguration AgentAuthenticationKey ALL_GROUPS	☒ ☒ ☒ ☒ ☒ ☐

Una lista de control de acceso especifica acciones válidas para cada recurso por separado para las identidades seleccionadas. Al crear una política centrada en recursos, especifique las acciones permitidas en cada recurso. No tiene que seleccionar acciones de un recurso determinado sólo porque sean válidas. Por ejemplo, puede permitir la creación de informes pero no permitir la creación de alertas, aunque la creación sea una acción válida para las alertas. La lista de control de acceso es la política más detallada al implementarla para una identidad cada vez.

Configuración de la lista de control de acceso									
Recursos			Acciones					Filtros	
Agregar recurso:			create						
			schedule						
			annotate						
			dataaccess						
						edit			
☐	Alert		☒	☒	☐	☐	☐		
☐	Data		☐	☐	☐	☒	☐		
☐	Database		☐	☐	☐	☐	☒		
☐	EventGrouping		☒	☐	☐	☐	☐		
☐	Integration		☒	☐	☐	☐	☒		
☐	Profile		☒	☐	☐	☐	☐		
☐	Report		☒	☒	☒	☐	☐		
☐	Tag		☒	☐	☐	☐	☐		
☐	AgentConfiguration		☐	☐	☐	☐	☒		
☐	AgentAuthenticationKey		☐	☐	☐	☐	☒		
☐	ALL_GROUPS		☐	☐	☐	☐	☒		
☐	Connector		☐	☐	☐	☐	☒		

Una lista de control de acceso a identidades especifica las acciones permitidas a las identidades seleccionadas en todos los recursos seleccionados aplicables. Al crear una política centrada en identidades, especifique qué identidades puede llevar a cabo cada acción (crear, programar, anotar, editar) en todos los recursos listados a los que hacen referencia las acciones. Si desea restringir la programación de alertas para los auditores, debe dejar en blanco la programación. Sin embargo, al dejar en blanco la programación, también evitará que los auditores puedan programar informes.

Configuración de la lista de control de identidad de acceso

Especificar/buscar identidades

Tipo:

▼

Buscar identidades

Identidad:

▼

Identities selected

Identities	Acciones
	create schedule annotate dataaccess edit
[Valor predeterminado]	☐ ☐ ☐ ☐ ☐
Administrator ▼	☒ ☒ ☒ ☒ ☒
Analyst ▼	☐ ☒ ☒ ☒ ☐
Auditor ▼	☐ ☐ ☒ ☒ ☐

Recursos

Alert

Database

EventGrouping

Integration

Profile

Report

Tag

AgentConfiguration

AgentAuthenticationKey

ALL GROUPS

▲

▼

▼

Recursos y acciones

Al crear políticas, configure una política de acceso para la que sea necesario un filtro de acceso. Un filtro de acceso es un filtro que el administrador puede emplear para controlar qué datos de eventos pueden visualizar los grupos o los usuarios que no son administradores. Por ejemplo, un filtro de acceso puede restringir los datos que aparecen en los informes visualizados por los grupos o los usuarios especificados. Los filtros de acceso se convierten de forma automática en políticas de obligación de EEM. Los filtros de acceso se suelen expresar en términos de rutas relativas para los objetos a los que se debe limitar el acceso de los usuarios. Puede visualizar estas rutas relativas en el área de carpetas de EEM de la interfaz.

Normalmente, las políticas que autorizan acciones como la creación y la programación se definen mediante clases de recursos de CALM y recursos de CALM como informes, etiquetas, archivos de asignación de datos y de análisis de mensajes, así como reglas de supresión y resumen. Las políticas que autorizan las acciones de lectura y escritura se definen mediante el tipo de recurso Objeto seguro y el recurso Objeto aplicación. La acción de edición es la única acción válida para los recursos relacionados con los agentes en el tipo de recurso de CALM.

En concreto, las acciones que se pueden autorizar para objetos pertenecientes al tipo de recurso de CALM son las siguientes:

Acción	Recurso	Descripción
Anotar	Report	Registro de comentarios sobre informes
Crear	EventForwarding	Creación de reglas para transferencia de eventos específicos a aplicaciones de terceros.
Crear	EventGrouping	Creación de reglas de supresión y resumen mediante la gramática de eventos comunes
Crear	Integration	Creación de archivos de asignación de datos y análisis de mensajes mediante la gramática de eventos comunes
Crear	Perfil	crear perfiles.
Crear	Report	Creación de informes y consultas
Crear	Tag	Creación de etiquetas para informes y consultas
Acceso a datos	Data	Acceso a datos de eventos de CALM, que se pueden limitar mediante filtros de acceso a datos.

Acción	Recurso	Descripción
Editar	AgentConfiguration	Creación de grupos de agentes Configuración de agentes instalados con recursos para la recopilación y el destino del procesamiento
Editar	AgentAuthenticationKey	Creación y edición de la clave de autenticación del agente que se especifica durante la instalación del agente
Editar	ALL_GROUPS	Edición de todos los grupos de agentes disponibles Nota: Se puede restringir el acceso a un grupo de agentes determinado mediante la especificación del nombre del grupo de agentes como recurso
Editar	Connector	Configuración de conectores
Editar	Database	Determinación de los registros existentes que coinciden con los criterios de consulta del catálogo de archivos y recatalogación de la base de datos
Editar	Integration	Edición de los detalles de la integración
Programar	Alert	Programación de alertas de acción
Programar	Report	Programación de informes y consultas

A continuación, se muestran las acciones que permiten a los usuarios ver o editar un objeto perteneciente al tipo de recurso Objeto seguro:

Acción	Recurso	Descripción
Leer	Objeto aplicación	Visualización de plantillas de informes, plantillas de consultas, etiquetas, tareas de informes programados, tareas de alertas, configuraciones de servicios, archivos de asignación de datos (DM), archivos de análisis de mensajes (XMP), así como reglas de supresión y resumen y reglas de transferencia de eventos.
Leer	Calendario	Visualización de los calendarios incluidos en Administración, Gestión de usuarios y accesos, Calendarios
Leer	Carpeta	Visualización de las carpetas incluidas en Administración, Gestión de usuarios y accesos, Carpetas de EEM

Acción	Recurso	Descripción
Leer	Usuario global	Visualización de la información mostrada para los usuarios listados al realizar una consulta de Usuarios globales en Administración, Gestión de usuarios y accesos, Usuarios
Leer	iPoz	Visualización de la configuración del almacén de usuarios en Administración, Gestión de usuarios y accesos, Almacén de usuarios Visualización de la configuración de las políticas de contraseñas en Administración, Gestión de usuarios y accesos, Política de contraseñas
Leer	Política	Visualización de las políticas incluidas en Administración, Gestión de usuarios y accesos, Políticas de acceso
Leer	Usuario	Visualización de los detalles del usuario al realizar una consulta de Detalles del usuario de la aplicación en Administración, Gestión de usuarios y accesos, Usuarios
Leer	Grupo de usuarios	Visualización de la pertenencia al grupo de aplicaciones de los usuarios listados al realizar una consulta de Detalles del usuario de la aplicación en Administración, Gestión de usuarios y accesos, Usuarios
Escribir	Objeto aplicación	Edición o supresión de plantillas de informes, plantillas de consultas, etiquetas, tareas de informes programados, tareas de alertas, configuraciones de servicios, archivos de asignación de datos (DM), archivos de análisis de mensajes (XMP), así como reglas de supresión y resumen y reglas de transferencia de eventos.
Escribir	Calendario	Edición de calendarios definidos por el usuario
Escribir	Carpeta	Edición de datos definidos por el usuario y añadidos a la estructura de carpetas de EEM
Escribir	Usuario global	Edición de los detalles del usuario global
Escribir	iPoz	Configuración de las políticas de contraseñas y del almacén de usuarios
Escribir	Política	Edición de las políticas predefinidas y definidas por el usuario
Escribir	Usuario	Edición de los detalles del usuario de la aplicación
Escribir	Grupo de usuarios	Creación, edición o eliminación de un grupo de usuarios de la aplicación

Recursos de CALM y carpetas de EEM

En todas las políticas de CALM personalizadas que incluyan EventForwarding, EventGrouping, Integration, Profile o Report que cree desde el principio, deberá crear una política de ámbito en AppObject. La política de ámbito cuenta con un acceso de lectura/escritura que filtra las rutas de EEM de cada recurso de CALM listado en la política de CALM correspondiente. Los mismos grupos que son las identidades de la política de CALM son los que se asignan como entidades de esta política. Para finalizar este conjunto de políticas, cree otra política de ámbito de sólo lectura, asigne una identidad que sólo pueda ver el recurso e introduzca un filtro con una ruta de carpeta de EEM.

Nota: Que la política de CALM requiera o no una política de ámbito de soporte depende del recurso que emplee la política de CALM. Por ejemplo, los recursos Database, Tag y Alert son recursos totalmente pertenecientes a CALM y no necesitan políticas de ámbito. Tampoco son necesarias políticas de ámbito para los recursos relacionados con agentes.

Puede ver las carpetas de EEM en la ficha Administración, en la subficha Gestión de usuarios y accesos. Cuando selecciona una carpeta como Supresión, se muestra esa ruta. Vea el ejemplo siguiente:



Carpets de EEM

- ▼ CALM_Configuration
 - ▶ Modules
 - ▼ Content
 - Library
 - ▼ Rules
 - Suppression**
 - Forwarding
 - Summarization
 - ▶ Reports
 - CEG
 - Mapping
 - Parsing
 - ▶ Profiles
 - flex
 - ▶ AgentManager
 - System
 - Calendars
 - Policies
 - Users
 - UserGroups

Detalles de la carpeta

Nombre	Ruta
Suppression	/CALM_Configuration/Content/Rules/Suppression

Especifique la ruta de la carpeta de EEM como valor en una expresión que comience por `pozFolder` CONTAINS, tal y como se indica en la sección Filtros de la definición de una política. A continuación, se muestra un ejemplo:

Filtros					
Lógica	(	Valor/tipo izquierdo	Operador	Valor/tipo derecho	)
NINGUNO	(	atributo con nombre pozFolder	STRING CONTAINS *..*	valor CALM_Configuration/M	)
O	(	valor pozFolder	STRING CONTAINS *..*	valor CALM_Configuration/M	)

Las tablas siguientes muestran directrices para el valor especificado en el filtro de una política de ámbito relacionada con una política de CALM que otorga o prohíbe el acceso a determinados recursos de CALM.

Nota: No existe una correspondencia única entre los recursos de CALM y las carpetas.

Creación de una política de ámbito que otorga acceso al contenido de este recurso de CALM **Adición de un filtro que especifica esta ruta de la carpeta de EEM**

EventForwarding	pozFolder CONTAINS /CALM_Configuration/Content/Rules/Forwarding
EventGrouping	pozFolder CONTAINS /CALM_Configuration/Content/Rules/Summarization pozFolder CONTAINS /CALM_Configuration/Content/Rules/Suppression
Integration (servidor)	pozFolder CONTAINS /CALM_Configuration/Content/Mapping pozFolder CONTAINS /CALM_Configuration/Content/Parsing
Perfil	pozFolder CONTAINS /CALM_Configuration/Content/Profiles
Report	pozFolder CONTAINS /CALM_Configuration/Content/CEG pozFolder CONTAINS /CALM_Configuration/Content/Reports

Creación de una política de ámbito que requiere acceso a este módulo de CALM **Adición de un filtro que especifica esta ruta de la carpeta de EEM**

Gestor de agentes	pozFolder CONTAINS /CALM_Configuration/Modules/AgentManager
Almacenamiento de registro de eventos	pozFolder CONTAINS /CALM_Configuration/Modules/logDepot

Creación de una política de ámbito que requiere acceso a este módulo de CALM **Adición de un filtro que especifica esta ruta de la carpeta de EEM**

Servidor de informes	pozFolder CONTAINS /CALM_Configuration/Modules/calmReporter
Módulo de suscripción	pozFolder CONTAINS /CALM_Configuration/Modules/Subscription

Recursos globales y funcionalidad de CA EEM

Puede crear una política de ámbito similar en cuanto a objetivos a la política de CALM, excepto que los recursos serán globales en lugar de específicos del producto. Los recursos globales son aquellos recursos que se emplean en múltiples productos de CA. Puede crear políticas que concedan o denieguen acceso a determinados recursos globales, a los que se puede acceder mediante botones de la ficha Administración, en la subficha Gestión de usuarios y accesos.

Utilice la tabla siguiente como guía al crear una política de ámbito que conceda o deniegue a determinadas identidades la capacidad de leer o escribir; el recurso especificado es un recurso global.

Tarea	Acción	Recurso global
Mostrar, crear, editar o eliminar un usuario global, un grupo global de usuarios y un grupo de usuarios de la aplicación (función); agregar un grupo de aplicaciones (función) a un usuario global o crear un usuario global con una función.	Leer y escribir	Usuario Grupo de usuarios Usuario global Grupo de usuarios globales
Crear, editar, copiar, exportar, desactivar, probar, visualizar o eliminar una política; agregar un calendario a una política	Leer y escribir	Política Calendario
Crear, editar, copiar, visualizar o eliminar un filtro de acceso; visualizar carpetas de EEM	Leer y escribir	Política
Crear un calendario	Leer y escribir	Calendario
Configurar el almacén de usuarios; crear, editar o visualizar políticas de contraseñas	Leer y escribir	iPoz

Al crear un filtro para un recurso global, consulte el filtro para la política de acceso a la aplicación de CALM a modo de ejemplo. Una de las acciones que lleva a cabo el filtro es la especificación de las acciones que corresponden a cada recurso. Si hace clic en Editar en una política predefinida, puede examinar el origen para obtener un ejemplo de cómo introducir la lógica.

Planificación de la función del usuario

Si los grupos de usuarios de la aplicación predefinidos (Administrator, Analyst y Auditor) no son suficientes para sus necesidades, puede crear funciones personalizadas con nuevos grupos de usuarios de la aplicación. Por ejemplo, para asignar un pequeño grupo de personas para gestionar las cuentas de usuario, en el caso de que dichas personas no tengan acceso a la funcionalidad no relacionada de CA Enterprise Log Manager, puede definir una función Administrador cuenta usuario, crear una política de ámbito para dicha función, agregar dicha función a la política de acceso a la aplicación de CALM, así como asignar dicha función a los usuarios que deban gestionar las cuentas de usuario.

La planificación de usuario para CA Enterprise Log Manager consta de los pasos siguientes:

- Determinación del número de usuarios necesarios para administrar, analizar y realizar auditorías de CA Enterprise Log Manager
- Identificación de los usuarios a los que se concederá acceso a CA Enterprise Log Manager

Si piensa en crear funciones personalizadas con políticas de acceso asociadas, tenga en cuenta este sistema:

- Identifique la función que desea asignar a cada usuario de CA Enterprise Log Manager
- Identifique el tipo de acceso a los recursos de CA Enterprise Log Manager que se necesita para cada función

También puede tener en cuenta las alternativas siguientes para las funciones definidas por el usuario (grupos de la aplicación):

- Configure políticas de grupos dinámicos de usuarios que crean grupos dinámicos de usuarios.
- Cree grupos globales y trátelos como a grupos de la aplicación, es decir, asígnelos a usuarios y asígnelos a políticas como identidades.

Este sistema puede resultar útil si se crean políticas con el objetivo de restringir el acceso por ubicación geográfica y si desea que los mismos usuarios tengan los mismos derechos en múltiples productos de CA. Por ejemplo, un grupo global de Location-A_Admin podría asignarse a usuarios que deban administrar varios productos de CA en Location-A. Podrían crearse políticas para cada producto de CA que garantizaran derechos administrativos a los servidores en los que se hubiera instalado dicho producto en Location-A.

Más información:

[Creación de grupos globales](#) (en la página 40)

Configuración de políticas de acceso y funciones de usuario personalizadas

Una *función del usuario* puede ser un grupo de usuarios de la aplicación predeterminado o un grupo de aplicaciones definido por el usuario. Es necesario contar con funciones de usuarios personalizadas cuando los grupos de la aplicación predeterminados (Administrator, Analyst y Auditor) no están lo suficientemente depurados como para reflejar las asignaciones de trabajo. Las funciones de usuarios personalizadas requieren el empleo de políticas de acceso personalizado y la modificación de las políticas predefinidas para incluir la función nueva.

Los administradores pueden crear funciones de usuario y sus correspondientes políticas del modo siguiente:

1. Para cada función asumida por usuarios de CA Enterprise Log Manager:
 - Identifique los recursos a los que se debe permitir el acceso.
 - Identifique las acciones que desea permitir en cada recurso.
 - Identifique las identidades o individuos a los que se aplica esta función.

Nota: Las identidades pueden ser otros grupos de la aplicación diseñados para formar un supergrupo.

2. Si un grupo de aplicaciones predefinido es demasiado amplio para sus necesidades, cree un nuevo grupo de aplicaciones y asigne dicho grupo a los individuos identificados. Es conveniente designar los grupos de aplicaciones definidos por el usuario con nombres que describan la función que deben llevar a cabo los usuarios asignados.
3. Agregue el nuevo grupo de aplicaciones a la política de acceso a la aplicación de CALM, que es un tipo de lista de control de acceso.
4. Si la función nueva debe ser capaz de llevar a cabo acciones en uno o varios recursos, como la acción de crear, lleve a cabo lo siguiente:
 - a. Configure una política de CALM que permita al nuevo grupo de aplicaciones crear o llevar a cabo otras acciones válidas en los recursos de CA Enterprise Log Manager identificados.
 - b. Configure una política de ámbito que conceda al nuevo grupo de aplicaciones acceso de lectura y escritura al recurso AppObject y especifique un filtro que establezca el lugar de almacenamiento del recurso identificado en las carpetas de EEM. Para cada filtro, introduzca el atributo mencionado, `pozFolder CONTAINS valor`, donde "valor" es la ruta de la carpeta de EEM que comienza por `/CALM_Configuration`.
5. Si la función nueva sólo necesita visualizar un determinado recurso de CA Enterprise Log Manager, configure una política de ámbito que permita un acceso de lectura a AppObject y especifique un filtro en la ubicación del atributo mencionado, `pozFolder, CONTAINS valor`, donde "valor" es la ruta de la carpeta de EEM que comienza por `/CALM_Configuration` en la ubicación donde está almacenado ese recurso.
6. Compruebe las políticas.
7. Asigne la función nueva a las cuentas de usuario.

Los administradores también pueden crear accesos de usuario restringidos mediante filtros de acceso. Si un determinado tipo de acceso restringido sólo se aplica a un individuo, puede omitir la asignación de esa persona a una función o a un grupo de aplicaciones. Para limitar el acceso de un usuario:

1. Cree un usuario pero no le asigne ninguna función.
2. Concédale acceso a la aplicación de CA Enterprise Log Manager añadiendo al usuario a la política de acceso a CALM.
3. Cree una política de ámbito que garantice un acceso de lectura o escritura a Objeto seguro y Objeto aplicación, y especifique un filtro en el que el atributo mencionado, `pozFolder`, sea igual al valor de la carpeta de EEM del recurso. Por ejemplo, si el recurso son informes, establezca el atributo mencionado, `calmTag`, con un valor igual al valor de la etiqueta del informe.
4. Cree un filtro de acceso personalizado.

Los administradores pueden personalizar el acceso de los usuarios a los recursos de CA Enterprise Log Manager. Observe los siguientes ejemplos:

- Cree funciones para asignar responsabilidades de administración específicas a diferentes grupos de administradores. Por ejemplo, cree una función como Administrador cuenta usuario. Cree una política que permita a los usuarios que tengan esta función acceder sólo a la funcionalidad necesaria para mantener los usuarios y los grupos. Una política de este tipo debe definir un acceso de lectura y escritura al recurso Usuario global, así como a los recursos Usuario y Grupo usuarios.
- Cree funciones para distribuir las responsabilidades de los analistas en los distintos tipos de informes y consultas basadas en etiquetas. Por ejemplo, puede crear funciones como Analista acceso al sistema y Analista PCI, y asignar a los analistas sólo una de las funciones de analistas restringidas. A continuación, cree políticas que confieran acceso a un subconjunto de estos recursos en función de las etiquetas. Por ejemplo, cree una política que permita que la función Analista acceso al sistema acceda a los informes y a las consultas que tengan la etiqueta de acceso al sistema, y otra política que permita que la función Analista PCI acceda a los informes y a las consultas que tengan la etiqueta de PCI. Cree otras funciones y políticas en función de otras etiquetas. Las políticas que restringen en acceso de este modo lo hacen mediante filtros de acceso.

Los administradores pueden crear políticas basadas en servidores a través de uno de los métodos siguientes:

- **Restricción de los datos**

Puede restringir el acceso a determinados registros mediante la creación de un filtro de acceso a datos, el establecimiento del filtro para el campo receiver_name y la especificación de un valor como systemstatus o syslog.

- **Restricción de la configuración**

Puede restringir el acceso a un determinado servidor de CA Enterprise Log Manager mediante la creación de una política en la clase de recurso Objeto seguro con Objeto aplicación como recurso seleccionado. Es decir, para restringir el acceso sólo a la configuración del servidor de informes de un host determinado, defina un filtro como se indica a continuación:

```
pozFolder contains /CALM_Configuration/Modules/calmReporter/LogServer01
```

Más información:

[Políticas de ejemplo para integraciones personalizadas](#) (en la página 146)

[Políticas de ejemplo para reglas de supresión y resumen](#) (en la página 148)

[Creación de un filtro de acceso](#) (en la página 111)

[Restricción del acceso a datos a un usuario: caso de Win-Admin](#) (en la página 125)

[Restricción de acceso a una función: caso de analista de PCI](#) (en la página 139)

Creación de un grupo de usuarios de la aplicación (función)

Puede crear un nuevo grupo de usuarios de la aplicación para admitir las funciones que necesita. Una vez que haya creado un nuevo grupo de usuarios de la aplicación, debe crear políticas de acceso para dicho grupo.

Un caso en el que no son necesarias nuevas políticas de acceso para un grupo nuevo es cuando dicho grupo pertenece a grupos existentes. Piense en el caso de que necesite una función para las personas que se dedican a crear asignaciones de datos y archivos de análisis de mensajes, una función para personas dedicadas a crear reglas de supresión y resumen, y una tercera regla para aquellas que pueden llevar a cabo ambas tareas. Puede definir un grupo de usuarios de la aplicación denominado AdminDMMP con una política que garantiza un acceso de creación al recurso Integration, y otro grupo denominado AdminSS con una política que garantiza un acceso de creación al recurso EventGrouping. A continuación, puede crear un tercer grupo denominado AdminDMMPSS perteneciente a los grupos AdminDMMP y AdminSS. Este tercer grupo asumirá automáticamente las políticas de los dos grupos a los que pertenece.

En lugar de crear nuevos grupos o funciones de la aplicación, puede ampliar las funciones de las funciones predefinidas Analyst y Auditor. Por ejemplo, si desea que los analistas puedan crear reglas de supresión y resumen y quiere que los auditores sean capaces de ver dichas reglas, puede crear una política de CALM que permita crear reglas de resumen y supresión, así como una política de ámbito que permita visualizar o editar reglas personalizadas y asignar la función Analyst a dichas políticas. A continuación, puede crear una política de ámbito que permita a los usuarios visualizar las reglas de supresión y resumen, así como asignar el grupo de auditor a dicha política.

Sólo los administradores pueden crear funciones nuevas.

Para crear un nuevo grupo de usuarios de la aplicación (función)

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Grupos.
3. Haga clic en el botón Nuevo grupo de aplicaciones situado a la izquierda de la carpeta Grupos de aplicaciones de la lista de grupos de usuarios.
4. Indique un nombre y una descripción del grupo.

5. Si ya ha definido que este grupo de usuarios nuevo debe tener acceso a dos o más grupos de la aplicación definidos por el usuario, seleccione dichos grupos de la aplicación para activar la pertenencia. Si no es así, no seleccione nada.

Nota: Si este nuevo grupo está formado por grupos existentes, las políticas existentes de cada uno de los grupos de componentes también se aplicarán a este grupo. No se requieren más políticas.

6. Haga clic en Guardar.
7. Haga clic en Cerrar.

Más información:

[Paso 2: Creación de la función de analista de PCI](#) (en la página 141)

[Políticas de ejemplo para reglas de supresión y resumen](#) (en la página 148)

Concesión de acceso a CA Enterprise Log Manager a funciones personalizadas

Al crear una función o un grupo de usuarios de la aplicación, asegúrese de agregarlos a la política de acceso a la aplicación de CALM predefinida. Sólo las identidades añadidas de forma explícita a esta política pueden acceder a CA Enterprise Log Manager. Las identidades pueden ser usuarios individuales o miembros de un grupo de usuarios.

Si se produce una situación en la que los usuarios asignados a un grupo de usuarios nuevo no pueden iniciar sesión en CA Enterprise Log Manager, compruebe que las identidades de la política de acceso a la aplicación de CALM incluyen a dicho grupo.

Para permitir el acceso a CA Enterprise Log Manager a un grupo de usuarios de la aplicación definido por el usuario

1. Seleccione la ficha Administración, haga clic en Gestión de usuarios y accesos y, a continuación, haga clic en Políticas de acceso en el panel de la izquierda.
2. Haga clic en Políticas de ámbito y seleccione el acceso a la aplicación de CALM.

3. En Identidades, busque el grupo de aplicaciones nuevo del modo siguiente:
 - a. Para Tipo, seleccione Grupo de aplicaciones.
 - b. Haga clic en Buscar identidades.
 - c. Deje Nombre como atributo y LIKE como operador. Haga clic en Buscar.
Aparece el nombre del grupo de aplicaciones nuevo en la lista de identidades que se muestra en pantalla.
 - d. Seleccione el nombre del nuevo grupo de aplicaciones y haga clic en el botón de movimiento para desplazar el nombre del grupo al cuadro Identidades seleccionadas.
4. Haga clic en Guardar.

Adición de identidades a una política existente

Cuando crea un grupo de usuarios de la aplicación nuevo, puede agregar dicho grupo a políticas existentes si procede. Al crear un usuario que no tiene ninguna función, pero que tiene acceso limitado mediante un filtro de acceso, puede agregar dicho usuario a las políticas existentes.

Importante: Al trabajar con las políticas de acceso instaladas, preste mucha atención para no eliminarlas, ya que no están bloqueadas ni protegidas.

Si se elimina de forma accidental una política de acceso predefinida, los usuarios no podrán acceder al servidor de CA Enterprise Log Manager hasta que no se restaure. Se pueden restaurar las políticas que utilizan la utilidad de safex.

Para agregar identidades a una política existente

1. Seleccione la ficha Administración, haga clic en Gestión de usuarios y accesos y, a continuación, haga clic en Políticas de acceso en el panel de la izquierda.
2. Haga clic en el tipo de política y, a continuación, seleccione la política que se aplica al nuevo grupo de usuarios de la aplicación. Visualice el panel Identidades.
3. Para Tipo, seleccione Grupo de aplicaciones.
4. Haga clic en Buscar identidades.
5. Deje Nombre como atributo y LIKE como operador. Haga clic en Buscar.
Aparece el nombre del grupo de aplicaciones nuevo en la lista de identidades que se muestra en pantalla.
6. Seleccione el nombre del nuevo grupo de aplicaciones y haga clic en el botón de movimiento para desplazar el nombre del grupo al cuadro Identidades seleccionadas.
7. Haga clic en Guardar.

Más información:

[Paso 4: Adición de analistas de PCI a políticas existentes](#) (en la página 142)

Creación de una política de acceso a CALM

Puede crear una política de acceso a CALM para conceder (o denegar) una o varias acciones válidas en uno o varios recursos de CALM.

Los recursos de CALM siguientes son específicos de la aplicación; es decir, que sólo los emplea el producto de CA Enterprise Log Manager:

- Alert
- AgentConfiguration
- AgentAuthenticationKey
- ALL_GROUPS
- Connector
- Data
- Database
- EventGrouping
- Integration
- Profile
- Report
- Tag

Para crear una política de CALM nueva desde el principio

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso.
3. Haga clic en el botón Nueva política de acceso situado a la izquierda de la carpeta de CALM.
4. Introduzca un nombre descriptivo para la política y, si lo desea, una breve descripción.
5. Si la política es temporal, seleccione Calendario con el intervalo de fechas aplicable.
6. Acepte CALM como nombre de clase de recurso.

7. Seleccione Tipo en el panel general en función de los criterios siguientes:
 - Seleccione una política de acceso para conceder o denegar a todas las identidades seleccionadas la capacidad de llevar a cabo todas las acciones seleccionadas en todos los recursos seleccionados a los que hacen referencia.
 - Seleccione una lista de control de acceso para conceder o denegar a todas las identidades seleccionadas la capacidad de llevar a cabo sólo las acciones seleccionadas en un recurso seleccionado.

Nota: No es posible guardar filtros de múltiples recursos. La solución alternativa es crear políticas independientes, una para cada combinación de recursos/filtros.

 - Seleccione una lista de control de acceso de identidades para conceder o denegar a todas las identidades seleccionadas la capacidad de llevar a cabo las acciones seleccionadas en todos los recursos seleccionados a los que hacen referencia.
8. Utilice el área de identidades para seleccionar los usuarios o los grupos a los que hace referencia esta política del modo siguiente:
 - a. Seleccione Grupo de aplicaciones como Tipo o una de las otras opciones, haga clic en Buscar identidades y haga clic en Buscar.
 - b. Seleccione las identidades entre las que están disponibles y haga clic en el botón de movimiento para desplazarlas al cuadro Identidades seleccionadas.
9. Si el tipo de política es una política de acceso, realice la configuración de la política de acceso del modo siguiente:
 - a. Introduzca un recurso de CALM en el campo de adición de recursos y haga clic en Agregar.
 - b. Seleccione las acciones que puedan llevar a cabo las identidades seleccionadas en los recursos seleccionados. Las acciones válidas incluyen las siguientes: anotar, crear, acceso a datos, editar y programar. No puede otorgar la capacidad de llevar a cabo una acción determinada en un recurso y no hacerlo en otro en el que es válida.

10. Si el tipo de política es una lista de control de acceso, lleve a cabo la configuración de la lista de control de acceso del modo siguiente:
 - a. Introduzca un recurso de CALM en el campo de adición de recursos y haga clic en Agregar.
 - b. Seleccione las acciones que puedan llevar a cabo las identidades seleccionadas en este recurso. Las acciones válidas incluyen una o varias de las acciones siguientes: anotar, crear, acceso a datos, editar y programar.
 - c. Repita los dos últimos pasos para cada recurso que desea asignar a esta política.

De este modo, puede permitir la realización de una acción, como la de crear, en un recurso sí y en otro no.
11. Si el tipo de política es una lista de control de acceso de identidades, lleve a cabo la configuración de la lista de control de acceso de identidades del modo siguiente:
 - a. Para cada identidad seleccionada, seleccione las acciones que se permitirán o se denegarán en todos los recursos para los que son válidas.
 - b. Para cada recurso que desee añadir, introduzca un nombre de recurso de CALM en el campo de adición de recursos y haga clic en Agregar:
12. Revise las casillas de verificación situadas en la parte superior y seleccione las que corresponda:
 - Seleccione Denegación explícita para cambiar la política de una que concede acceso a una que lo deniega.
 - Seleccione Desactivado para desactivar esta política de forma temporal si es nueva.
 - Seleccione Pre-implantación y, a continuación, seleccione Asignar etiquetas y agregue las etiquetas si emplea esta política para realizar pruebas y desea categorizar las políticas con etiquetas personalizadas.
13. Haga clic en Guardar y, a continuación, haga clic en Cerrar en el panel izquierdo.

Creación de política de ámbito

Puede crear una política de ámbito en cualquier recurso global. Las acciones de las políticas de ámbito se limitan a las de lectura y escritura.

- Muchos productos de CA (aplicaciones) emplean los recursos globales siguientes:
 - Calendario
 - Usuario global
 - Grupo de usuarios globales
 - iPoz
 - Política
 - Usuario
 - Grupo de usuarios
 - Objeto aplicación
- El recurso global Objeto aplicación le permite crear políticas de ámbito en módulos y recursos específicos de la aplicación. Esto se lleva a cabo a través de la adición de un filtro que designa la carpeta de EEM relevante en la que se almacena el módulo o el contenido específico de la aplicación.
 - Las carpetas de contenido de EEM que puede emplear en filtros con el recurso Objeto aplicación incluyen las siguientes:
 - EventGrouping
 - Integration (servidor)
 - Perfil
 - Report
 - Las carpetas del módulo de CA Enterprise Log Manager que puede emplear en filtros con el recurso Objeto aplicación incluyen las siguientes:
 - Almacenamiento de registro de eventos
 - Servidor de informes
 - Suscripción

Puede crear una política desde el principio si no existe ninguna a partir de la que ajustar la configuración. Si crea una política de ámbito asociada a una política de CALM que ha creado, especifique las mismas entidades que las de la política de CALM relacionada.

Sólo los administradores pueden crear, editar, suprimir y visualizar políticas de acceso.

Para crear una nueva política de ámbito de concesión explícita

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso.
3. Haga clic en el botón Nueva política de ámbito a la izquierda de la carpeta Políticas de ámbito.
4. Cree un nombre que designe a la política. Por ejemplo, incluya la función o funciones y las tareas a las que se aplica. Visualice los nombres de las políticas predeterminadas para los ejemplos de cómo puede utilizarse esta norma.
5. Introduzca una descripción corta que describa con precisión lo que implica el nombre más cifrado.
6. Normalmente se aceptará SafeObject como nombre de clase de recurso.
7. Seleccione Tipo en el panel general de acuerdo con los siguientes criterios:
 - Seleccione la política de acceso para conceder o denegar a todas las identidades seleccionadas la capacidad de realizar todas las acciones seleccionadas en todos los recursos seleccionados a los que se aplican.
 - Seleccione la lista de control de acceso para conceder o denegar a todas las identidades seleccionadas la capacidad de realizar sólo las acciones seleccionadas en un recurso seleccionado.

Nota: No es posible guardar filtros para varios recursos. La solución alternativa es crear políticas independientes, una para cada combinación recurso/filtros.

 - Seleccione la lista de control de acceso de identidades para conceder o denegar a cada identidad seleccionada la capacidad de realizar las acciones seleccionadas en todos los recursos seleccionados a los que se aplica.
8. Si el tipo de política es una lista de control de acceso o una política de acceso, utilice el área Identidades para seleccionar los usuarios o grupos a los que se aplica esta política.
 - a. Seleccione Grupo de aplicaciones para tipo, haga clic en Buscar identidades y luego en Buscar.
 - b. Seleccione identidades de las que estén disponibles y haga clic en el botón Mover para moverlas a la casilla Identidades seleccionadas.

9. Si el tipo de política es una política de acceso, todas las acciones se seleccionan para todos los recursos de forma predeterminada. Para personalizarla, complete la configuración de la política de acceso de la siguiente forma:
 - a. Seleccione un recurso de la lista desplegable Agregar recurso y haga clic en Agregar.
 - Seleccione AppObject si los recursos para los que se va a configurar el acceso de lectura o escritura son recursos específicos de CA Enterprise Log Manager.
 - Seleccione Usuario y Usuario global para acceder a los botones Usuarios en la ficha Administración, subficha Gestión de usuarios y accesos.
 - Seleccione Grupo de usuarios y Grupo de usuarios globales para acceder a los botones Grupos en la ficha Administración, subficha Gestión de usuarios y accesos.
 - Seleccione Política para acceder a los botones Políticas de acceso, Carpetas de EEM y Probar políticas en la ficha Administración, subficha Gestión de usuarios y accesos.
 - Seleccione Calendario para acceder al botón Calendarios en la ficha Administración, subficha Gestión de usuarios y accesos.
 - Seleccione iPoz para acceder a los botones Política de contraseñas y Almacén de usuarios en la ficha Administración, subficha Gestión de usuarios y accesos.
 - b. Seleccione leer para conceder/denegar acceso de vista; seleccione escribir para conceder/denegar acceso de edición. Si no selecciona ninguna acción, se seleccionarán todas.

Nota: Para conceder/denegar la creación de accesos, debe definir una política de acceso de CALM y seleccionar recursos de CA Enterprise Log Manager individualmente.
 - c. Agregue un filtro genérico que se aplique a los recursos seleccionados, si fuese necesario.

10. Si el tipo de política es una lista de control de acceso, complete la configuración de la lista de control de acceso de la siguiente forma:
- a. Seleccione un recurso de la lista desplegable Agregar recurso y haga clic en el botón Agregar (+).
 - b. Seleccione leer, escribir o ambos en Acciones.
 - c. Haga clic en el botón Editar filtros para abrir el formulario de filtros. Cree un filtro para el recurso asociado seleccionando o introduciendo valores para el valor/tipo Izquierda, valor/tipo Operador y valor/tipo Derecha.
 - d. Si el filtro incluye un nombre de recurso como un valor, seleccione la casilla de verificación con la etiqueta Tratar nombres de recursos como expresiones regulares. De lo contrario, deje esta casilla de verificación sin marcar.

Importante: Defina una política para cada combinación de filtro/recurso.

11. Si el tipo de política es una lista de control de acceso de identidad, complete la configuración de la lista de control de acceso de identidad de la siguiente forma:
- a. Para Tipo, seleccione una de las acciones que se muestran. Por ejemplo, seleccione Grupo de aplicaciones, haga clic en el vínculo Buscar identidades y haga clic en el botón Buscar para mostrar los miembros del tipo que ha seleccionado.
 - b. Seleccione las identidades y haga clic en el botón Mover para rellenar el panel Identidades seleccionadas.
 - c. Para cada identidad seleccionada, especifique lectura o escritura, o ambas.

Las acciones específicas de identidad se aplican a todos los recursos seleccionados. Es decir, una identidad determinada puede ver, ver y editar o sólo editar todos los recursos seleccionados.
 - d. Agregue los recursos a los que desee conceder/denegar las acciones específicas de la identidad.

12. Revise las casillas de verificación y seleccione las que se apliquen:

- Seleccione Denegación explícita para cambiar la política de una que concede acceso a una que deniega acceso.
- Seleccione Desactivado para deshabilitar esta política temporalmente, si es nueva.
- Seleccione Implementación previa y, a continuación, seleccione Asignar etiquetas y agregue las etiquetas si se está usando esta política con fines de prueba y desea categorizar las políticas con etiquetas personalizadas.

13. Haga clic en Guardar y, a continuación, en Cerrar en el panel izquierdo.

Más información:

[Paso 3: Creación de una política de acceso al sistema de Win-Admin](#) (en la página 129)

Creación de una política basada en una política existente

Puede crear una política de acceso nueva copiando una política de acceso existente y modificando la copia. Este procedimiento puede ahorrarle el tiempo que supone duplicar manualmente las especificaciones de una política existente que sólo requiere pequeños cambios para satisfacer los requisitos actuales.

Los administradores son los únicos que pueden crear, editar, eliminar o visualizar las políticas de acceso.

Para crear una política basada en una política existente

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso.
3. Seleccione CALM o las políticas de ámbito en función del tipo de política que desee utilizar como plantilla.
4. Haga clic en el vínculo del nombre para abrir la política que desea copiar.
5. Haga clic en Guardar como.

Aparece el cuadro de diálogo de solicitud de exploración.

6. Introduzca el nombre de la política nueva que se basará en la política abierta y haga clic en Aceptar.
7. Realice las modificaciones necesarias.

Por ejemplo, sustituya la identidad copiada por el nombre de la función (grupo de usuarios de la aplicación definido por el usuario) a la que se aplica esta política. Puede modificar las acciones permitidas en los recursos copiados. Puede hacer clic en Filtros y especificar otro filtro para la función nueva.
8. Haga clic en Guardar y, a continuación, en Cerrar.
9. Compruebe la definición de la política nueva.
 - a. Vuelva a seleccionar el tipo de política para mostrar en pantalla todas las políticas.
 - b. Compare la nueva política con la política original y verifique que todos los cambios deseados se reflejan en la política nueva.
 - c. Haga clic en Cerrar.
10. Compruebe la política.

Más información:

[Paso 5: Creación de políticas basadas en políticas de edición y visualización de informes de analistas](#) (en la página 143)

Comprobación de una política nueva

Puede comprobar si una política nueva es sintácticamente correcta mediante la función de comprobación de políticas. La función de comprobación de políticas le permite ejecutar consultas ad-hoc en las políticas de acceso que defina. Puede considerar un permiso como una solicitud: "Can {identity} perform {action} against the resource of type {resource class} and of name {resource} [with the following attributes]] [at the {specified time}]?". Un resultado ALLOW indica que la identidad introducida puede llevar a cabo la acción especificada en el recurso indicado con los atributos definidos y en el tiempo establecido.

Antes de comenzar, tenga a mano la política.

Para comprobar una política

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Probar políticas.
Aparece la página de parámetros de comprobación de permisos.
3. Si la política que quiere comprobar es una política en la que ha seleccionar una implementación previa y a añadido etiquetas, entonces seleccione la casilla de verificación que indica que desea incluir políticas de implementación previa y agregarlas etiquetas asociadas.
4. Rellene los campos de entrada: Si la política incluye filtros, especifique los filtros en el orden en el que aparecerán en la política.
5. Haga clic en Ejecutar comprobación de permiso.
6. Estudie el resultado y lleve a cabo una de las acciones siguientes:
 - Si el resultado es ALLOW, inicie sesión en CA Enterprise Log Manager como uno de los usuarios especificados como identidad en esta nueva política y compruebe la eficacia, el alcance y la cobertura de ésta estableciéndola en modo de uso de producción.
 - Si el resultado es DENY, verifique los datos introducidos en la consulta. Si son correctos, devuelva la política o realice las correcciones necesarias allí.

Creación de políticas de grupos dinámicos de usuarios

Los *grupos dinámicos de usuarios* constan de usuarios globales que comparten uno o varios atributos. Los grupos dinámicos de usuarios se crean mediante una política de grupo dinámico de usuarios en la que el nombre del grupo dinámico de usuarios y la pertenencia se basan en un conjunto de filtros configurados en los atributos de los usuarios y del grupo.

Puede crear un grupo dinámico formado por usuarios, grupos de aplicaciones, grupos globales o grupos dinámicos. Por ejemplo, puede crear un grupo dinámico de grupos globales o grupos de aplicaciones basado en el nombre, la descripción o la pertenencia a un grupo. También puede crear un grupo dinámico de usuarios con diferentes funciones basado en un atributo común de su perfil de usuario global, por ejemplo:

- Puesto
- Departamento u oficina
- Ciudad, estado o país

El administrador es el único que puede crear políticas de grupos dinámicos de usuarios.

Para crear políticas de grupos dinámicos de usuarios

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso.
3. Haga clic en Nueva política de grupos dinámicos
Aparece la página Nueva política de grupos dinámicos.
4. En el campo del nombre, introduzca un nombre de grupo que indique lo que tienen en común los usuarios de dicho grupo. Puede añadir una descripción.
5. Seleccione un tipo de política. El valor predeterminado es una política de acceso.

6. Seleccione las identidades del modo siguiente:
 - a. Para el tipo, seleccione Usuario, Grupo de aplicaciones, Grupo global o Grupo dinámico y haga clic en Buscar entidades.
 - b. Para el atributo, el operador y el valor, introduzca la expresión que establezca los criterios de pertenencia a este grupo y haga clic en Buscar.

 Por ejemplo, si ha seleccionado Usuario, puede introducir Puesto Like Gestor y hacer clic en Buscar para mostrar todos los usuarios cuyo puesto sea Gestor.
 - c. Seleccione en las identidades mostradas aquellas que vayan a ser miembros de este grupo dinámico y haga clic en la flecha de desplazamiento para trasladar las selecciones al cuadro Identidades seleccionadas.
7. Para las acciones, seleccione la pertenencia.
8. En el campo de adición de recursos, introduzca el valor que indicó en el campo Nombre y haga clic en el botón Agregar. Esto quiere decir que las identidades seleccionadas pertenecen al recurso de grupos dinámicos que acaba de crear.
9. También puede añadir más filtros.
10. Haga clic en Guardar.
11. Haga clic en el enlace de políticas de grupos dinámicos de usuarios y compruebe el grupo dinámico de usuarios que ha creado. Por ejemplo:

Directivas de grupos dinámicos de usuarios					
<< < 1 > >>					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identidades	Acciones	Recursos
Non-Administrators	SafeDynamicUserGroup	Concesión explícita	ug:Analyst ug:Auditor ug:CALM-Analyst ug:ResourceAccessAnalyst	belong	Non-Administrators
QA Group	SafeDynamicUserGroup	Concesión explícita	User1 User2 User3	belong	QA Group
Security Officers	SafeDynamicUserGroup	Concesión explícita	Administrator1 User3	belong	Security Officers

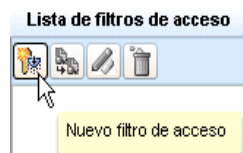
Creación de un filtro de acceso

Puede crear un filtro de acceso para restringir el acceso a los datos de registro que cumplan con los criterios de filtrado. De forma predeterminada, todos los usuarios de la aplicación de CA Enterprise Log Manager tienen acceso de consulta a los datos de registro de eventos guardados en los sistemas de almacenamiento de registro de eventos del servidor de CA Enterprise Log Manager activo, los servidores equivalentes en una federación combinada o los servidores descendientes en una federación jerárquica.

Puede restringir el acceso al sistema de almacenamiento de registro de eventos de uno o varios servidores de CA Enterprise Log Manager determinados mediante la creación de un filtro de acceso a datos. Puede aplicar filtros de acceso a un usuario individual o a un grupo.

Para crear filtros de acceso para funciones definidas por el usuario

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Nuevo filtro de acceso.

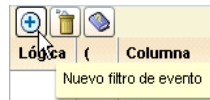


Aparece el asistente de diseño del filtro de acceso.

3. Para Detalles, introduzca el nombre y la descripción del filtro.
4. Haga clic en Identidades. Seleccione un tipo de identidad, haga clic en el botón de búsqueda para mostrar las identidades disponibles y utilice el control de cambio para seleccionar las identidades a las que se aplica este filtro de acceso.

Por ejemplo, seleccione el grupo de aplicaciones creado con este objetivo.

5. Establezca los filtros de acceso.
 - a. Haga clic en Filtros de acceso.
 - b. Haga clic en el botón Nuevo filtro de evento.



- c. Agregue una o más expresiones que definan el filtro de acceso.
 - d. Haga clic en Guardar y cerrar.Aparece el filtro de acceso que ha creado.
6. Haga clic en Cerrar.

Más información:

[Paso 4: Creación de un filtro de acceso a datos de Win-Admin](#) (en la página 133)
[Creación de un grupo de usuarios de la aplicación \(función\)](#) (en la página 95)

Mantenimiento de cuentas de usuario y políticas de acceso

Como administrador, puede llevar a cabo las siguientes tareas de mantenimiento en las cuentas de usuario y las políticas de acceso:

- Bloquear una cuenta de usuario para que el usuario no pueda iniciar sesión en CA Enterprise Log Manager
- Desbloquear las cuentas de usuario que se hayan bloqueado si la política de contraseñas no permite a ningún usuario desbloquear una cuenta de usuario bloqueada
- Agregar cuentas de usuario nuevas
- Editar cuentas de usuario existentes
- Bloquear o eliminar cuentas de usuario pertenecientes a personas que ya no necesitan acceso a CA Enterprise Log Manager
- Editar las políticas de acceso existentes
- Eliminar las políticas de acceso que ya no sean necesarias
- Crear, editar o eliminar políticas de delegación
- Crear, editar o eliminar filtros de acceso con sus correspondientes políticas de obligación generadas automáticamente
- Crear una superfunción a partir de las funciones existentes con acceso limitado
- Agregar una nueva función personalizada y sus correspondientes políticas de acceso

Creación de un calendario

Puede crear un calendario nuevo para ayudar a restringir el acceso de usuarios durante determinados períodos de tiempo. El calendario funciona como parte de las políticas de acceso. Al definir un calendario, puede incluir o excluir bloques de tiempo en horas, días de la semana o fechas.

Para crear un calendario

1. Haga clic en la ficha Administración, haga clic en Gestión de usuarios y accesos y, a continuación, haga clic en el botón de calendarios.
Aparece la página de calendarios.
2. Haga clic en el icono de nuevo calendario en la parte superior izquierda de la lista de calendarios.
Aparece el panel de detalles del calendario nuevo.
3. Introduzca un nombre que especifique la política de destino y proporcione una descripción del uso previsto.
4. Utilice los iconos del calendario para establecer fechas de inicio y finalización en el calendario.
5. Haga clic en Agregar inclusión de bloque de tiempo o Agregar exclusión de bloque de tiempo para crear períodos de excepción dentro del período de vigencia principal del calendario.
6. Haga clic en Guardar y, a continuación, en Cerrar.

Más información:

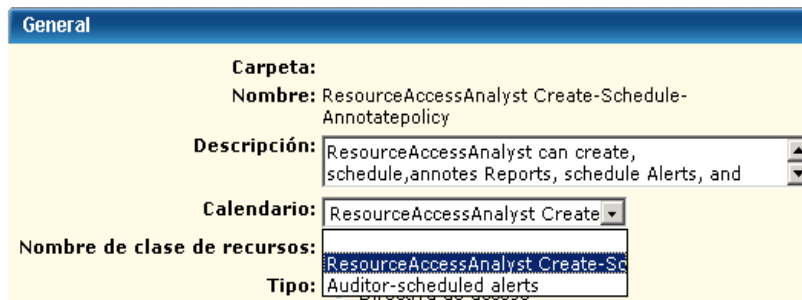
[Adición de un calendario a una política](#) (en la página 115)

Adición de un calendario a una política

Al crear una política, puede seleccionar un calendario existente que especifica la fecha en que las identidades especificadas pueden llevar a cabo las acciones seleccionadas en los recursos indicados. El calendario puede definir las fechas de inicio y finalización y los bloques de tiempo en horas o días de la semana.

Para agregar un calendario a una política

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Abra la política a la que desea aplicar el calendario.
 - a. Haga clic en Políticas de acceso.
 - b. Seleccione el tipo de política.
 - c. Seleccione la política.
3. Abra la lista desplegable de calendarios y seleccione el calendario creado para esta política.



General

Carpeta:

Nombre: ResourceAccessAnalyst Create-Schedule-Annotatepolicy

Descripción: ResourceAccessAnalyst can create, schedule,annotes Reports, schedule Alerts, and

Calendario: ResourceAccessAnalyst Create

Nombre de clase de recursos: ResourceAccessAnalyst Create-Schedule-Annotatepolicy

Tipo: Auditor-scheduled alerts

4. Haga clic en Guardar para guardar la adición del calendario a una política existente.

Más información:

[Creación de un calendario](#) (en la página 113)

Ejemplo: Limitar el acceso a los días laborables

Puede restringir la hora del día o los días de la semana que un determinado grupo de usuarios tiene acceso a CA Enterprise Log Manager a través de la creación de un calendario con los horarios de concesión de acceso, la creación de una función personalizada, la creación de una política nueva basada en la política que ofrece acceso a CA Enterprise Log Manager, así como mediante la asignación de un calendario y una función personalizada a esta política.

Ejemplo: Limitar el acceso a CA Enterprise Log Manager de los auditores externos a los días de la semana

Para limitar el acceso a CA Enterprise Log Manager de determinados grupos a los días laborables, cree un calendario para los días de la semana y añádalo a las políticas que ofrecen acceso específico a los auditores.

Por ejemplo, si desea limitar el acceso a CA Enterprise Log Manager de los auditores externos al horario de oficina, cree un calendario que especifique los días de la semana, de lunes a viernes, de 9:00 h a 17:00 h, durante todos los meses del año.

General

Carpeta:

Nombre: Weekdays 9-5

Descripción:

Inicio efectivo: lunes, 17 de noviembre de 2008 13:00:29

Detención efectiva: jueves, 31 de diciembre de 2009 17:00:00

Bloques de tiempo incluidos

Nuevo

Nombre: Nuevo

Hora de inicio: 00 : 00 Duración: 00 : 00

Intervalo de tiempo de repetición: 00 : 00

☒ = Seleccionado

Máscara de día de la semana

Dom	Lun	Mar	Mié	Jue	Vie	Sáb

Máscara de mes y día

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	ÚLTIMO			

Máscara de mes

ENERO	FEBRERO	MARZO
ABRIL	MAYO	JUNIO
JULIO	AGOSTO	SEPTIEMBRE
OCTUBRE	NOVIEMBRE	DICIEMBRE

Cree una función para auditores externos.

General

Carpeta: /UserGroups

Nombre: External Auditors

Descripción:

Miembros del grupo de aplicación

Grupos de usuarios disponibles	Grupos de usuarios seleccionados
Administrator Analyst Auditor	

Abra la política de ámbito de acceso a la aplicación de CALM y guárdela como política de acceso a la aplicación de CALM para auditores externos, seleccione el calendario de días laborables de 9 a 17 y seleccione el grupo de usuarios de auditores externos como identidad.

General

Carpeta:
Nombre: ExternalAuditors-CALM Application Access

Descripción: This policy defines who all can access the CALM Application

Calendario: Weekdays 9-5

Nombre de clase de recursos: SafeObject

Tipo: ☒ Directiva de acceso
☐ Lista de control de acceso
☐ Lista de control de identidad de acceso

Identidades

Especificar/buscar identidades **Identidades seleccionadas**

Tipo: Usuario **Buscar identidades** [Grupo] External Auditors

Importante: Utilice la función de calendario sólo con políticas que concedan acceso. No la utilice con políticas que deniegan acceso.

Más información:

[Creación de un calendario](#) (en la página 113)

[Creación de un grupo de usuarios de la aplicación \(función\)](#) (en la página 95)

[Creación de una política basada en una política existente](#) (en la página 106)

[Adición de un calendario a una política](#) (en la página 115)

Exportación de políticas de acceso

Puede exportar todas las políticas de un tipo seleccionado en cualquier momento, tanto las políticas predefinidas como las políticas personalizadas. La exportación de políticas es un buen método para mantener una copia de seguridad actualizada.

Una exportación crea un archivo XML para cada política seleccionada y todos los archivos XML se comprimen en un archivo denominado CAELM[1].xml.gz.

Para exportar políticas de acceso

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso.
3. Seleccione el tipo de política de acceso que desea exportar y haga clic en Exportar.

Aparecerá el cuadro de diálogo de descarga de archivos.

4. Haga clic en Guardar y guarde el archivo con un nombre único.
5. Haga clic en Cerrar.

Más información:

[Copia de seguridad de todas las políticas de acceso](#) (en la página 65)

Supresión de políticas personalizadas

Puede eliminar una política personalizada por cualquiera de los motivos siguientes:

- Que la haya guardado con un nombre distinto y no prevea realizar más cambios, así que debe eliminar el duplicado.
- Que ya no existan pertenencias activas en las identidades definidas para la política, por lo que la política ya no esté en uso.

Importante: Tenga cuidado de no eliminar una política predefinida. Si esto ocurriera, puede restaurarla si exportó una copia de seguridad.

Para eliminar políticas personalizadas

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Políticas de acceso.
3. Seleccione CALM o las políticas de ámbito en función del tipo de política que desee eliminar.
4. Haga clic en el nombre de la política que desea eliminar.
5. Haga clic en Suprimir.
6. Haga clic en Aceptar para confirmar la eliminación.

Eliminación de filtros de acceso y políticas de obligación

Puede eliminar un filtro de acceso y la política de obligación generada por el filtro para suprimir la limitación del acceso a datos.

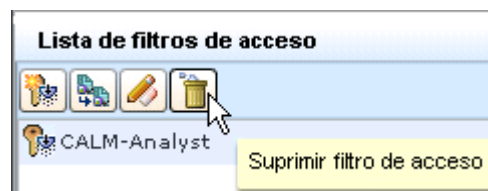
No elimine la política de obligación generada por el filtro desde las políticas de acceso.

Para eliminar filtros de acceso y sus políticas de obligación

1. Haga clic en la ficha Administración y haga clic en Gestión de usuarios y accesos.

La lista de filtros de acceso aparece en la parte superior del panel izquierdo.

2. Seleccione el filtro que desea eliminar y haga clic en el botón Suprimir filtro de acceso.



Aparece el mensaje de advertencia Confirmación de supresión de filtro de acceso.

3. Haga clic en Sí para eliminar el filtro de acceso seleccionado y la política de obligación asociada.

Ejemplo: Permitir a un usuario que no es administrador gestionar acciones de almacenamiento

Supongamos que desea permitir la gestión del almacenamiento automático a un grupo que no posee la función Administrator. Puede crear un grupo llamado AdministradorAlmacenamiento, una política de CALM que permite editar la base de datos de recursos. Esto ofrece un acceso de lectura al catálogo de archivos de la base de datos para realizar consultas, acceso de escritura al catálogo de archivos para llevar a cabo recatalogaciones, así como la posibilidad de emplear la utilidad LMArchive para realizar un almacenamiento manual o el script shell restore-ca-elm para restaurar bases de datos almacenadas de forma automática.

Para permitir a usuarios que no son administradores gestionar acciones de almacenamiento

1. Cree una función llamada AdministradorAlmacenamiento.
 - a. Seleccione la ficha Administración y, a continuación, la subficha Gestión de usuarios y accesos.
 - b. Seleccione Grupos.
 - c. Haga clic en Nuevo grupo de aplicaciones.
 - d. Introduzca AdministradorAlmacenamiento como nombre.
 - e. Haga clic en Guardar.

Se crea el grupo de aplicaciones o la función AdministradorAlmacenamiento.
 - f. Haga clic en Cerrar.

2. Cree una política de CALM para permitir un acceso de edición al recurso de la base de datos.
 - a. Haga clic en Políticas de acceso.
 - b. Haga clic en Nueva política de acceso para crear una política de CALM nueva.
 - c. Introduzca la política AdministradorAlmacenamiento en el campo Nombre.
 - d. Establezca que AdministradorAlmacenamiento pueda ejecutar la utilidad LMArchive y el script shell restore-ca-elm para la descripción.
 - e. Para las identidades, seleccione Grupo de aplicaciones como Tipo, haga clic en Buscar identidades y, a continuación, haga clic en Buscar.
 - f. Seleccione AdministradorAlmacenamiento y, a continuación, haga clic en la flecha de desplazamiento.
 - g. Introduzca Base de datos en el campo de adición de recursos y haga clic en Agregar.
 - h. Seleccione la edición como acción.

- i. Haga clic en Guardar. Haga clic en Cerrar.
3. Compruebe la política y verifique que el resultado es ALLOW.

Resultado	Directiva	Identidad	Clase de recurso	Recurso	Acción
PERMITIR	ArchiveAdministrator policy	ug:ArchiveAdministrator	CALM	Database	edit

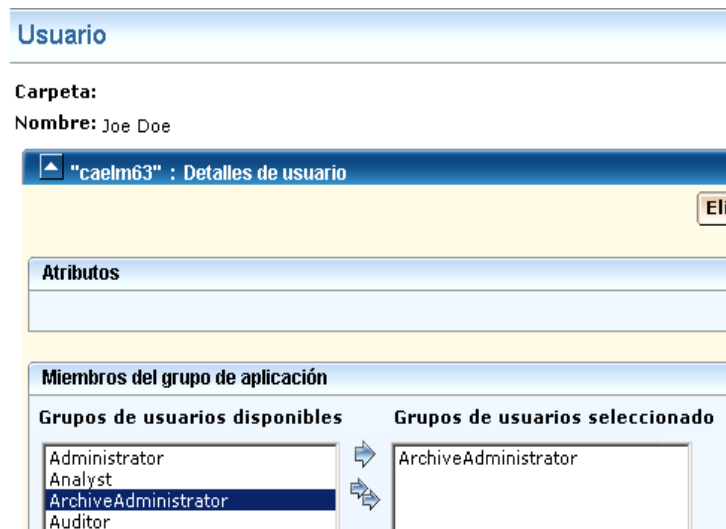
4. Conceda a la función AdministradorAlmacenamiento la posibilidad de iniciar sesión en CA Enterprise Log Manager.
 - a. Haga clic en CALM en Políticas de acceso.
 - b. Seleccione el acceso a la aplicación de CALM.
 - c. En Identidades, busque la función AdministradorAlmacenamiento del grupo de aplicaciones y desplácela a Identidades seleccionadas.



- d. Haga clic en Guardar. Haga clic en Cerrar. Haga clic en Cerrar.

Aparece la ficha Gestión de usuarios y accesos con los botones en el panel izquierdo.
5. Asigne la función AdministradorAlmacenamiento a uno o varios usuarios.
 - a. Haga clic en Usuarios.
 - b. Introduzca el nombre de una persona a la que desee asignar esta función como valor en Buscar usuarios y haga clic en Ir.

El nombre del usuario seleccionado aparece en la carpeta Usuarios.
 - c. Seleccione el vínculo del usuario seleccionado.
 - d. Haga clic en Agregar detalles del usuario de la aplicación.
 - e. Desplace el administrador de archivos a la lista de grupos de usuarios seleccionados.



- f. Haga clic en Guardar. Haga clic en Cerrar.
 - g. Repita esta acción con cada usuario al que desee asignar esta función.
 - h. Haga clic en Cerrar.
6. (Opcional) Revise los resultados desde CA Enterprise Log Manager.
- a. Haga clic en Cerrar sesión para cerrar sesión como administrador.
 - b. Inicie sesión como un usuario al que ha asignado la función AdministradorAlmacenamiento.
 - c. Haga clic en la ficha Administración y en la subficha Recopilación de servicios.
 - d. Seleccione Consulta de catálogo de archivos.
 - e. Compruebe que utiliza los botones Consulta y Recatalogar.
7. (Opcional) Ejecute el script de restauración restore-ca-elm con las credenciales del usuario definido en la función AdministradorAlmacenamiento para comprobar que la política funciona como esperaba.

Más información:

[Restauración de archivos almacenados de forma automática](#) (en la página 213)

Restricción del acceso a datos a un usuario: caso de Win-Admin

Puede limitar los informes que pueden visualizar los usuarios a aquellos que cuenten con una determinada etiqueta. Puede limitar los datos que pueden ver los usuarios en dichos informes a aquellos datos generados desde orígenes de eventos especificados. La limitación del acceso a informes con una etiqueta determinada se lleva a cabo mediante una política de acceso. La limitación del acceso a datos a eventos enviados a un servidor de CA Enterprise Log Manager determinado se lleva a cabo mediante un filtro de acceso. Al definir un filtro de acceso, la asignación de funciones es opcional. Es decir, que puede crear un usuario nuevo, no asignarle ninguna función y limitar el acceso a datos de dicho usuario mediante un filtro de acceso.

Tomemos como ejemplo la empresa ABC con cuatro centros de datos en EE. UU. El administrador quiere que el administrador de Windows del área de Houston tenga acceso de lectura a los eventos de Windows procesados por el controlador de dominios del área de Houston. Los eventos de Windows procesados por el servidor de CA Enterprise Log Manager instalado en el controlador de dominios de Houston se envían desde orígenes en los que los nombres de host comienzan por la cadena ABC-HOU-WDC.

Este ejemplo indica cómo crear un usuario denominado Win-Admin y garantizar que dicho usuario sólo pueda ver informes con la etiqueta de acceso al sistema, así como que los datos de dichos informes se limiten a eventos de orígenes de eventos con nombres de host que comiencen por la convención de nombres determinada.

El ejemplo ofrece detalles de cada uno de los pasos siguientes:

1. Cree el usuario nuevo, Win-Admin.
2. Otorgue a Win-Admin un acceso básico a CA Enterprise Log Manager. Agregue esta identidad a la política de acceso a la aplicación de CALM.
3. Restrinja el acceso de Win-Admin a los informes etiquetados como acceso al sistema. Cree una política de ámbito con acceso de lectura a AppObject y con filtros que especifiquen la carpeta de EEM en la que se almacenan los informes, y especifique que calmTag es igual al acceso al sistema. Compruebe la política.
4. Limite los datos que puede visualizar Win-Admin a aquellos generados por el controlador de dominios del área de Win-Admin. Cree un filtro de acceso, denominado Acceso a datos de Win-Admin, que limite las consultas y los datos de informes que puede visualizar Win-Admin a los eventos de Windows procedentes de orígenes de eventos con un nombre de host que comience por ABC-HOU-WDC.
5. Inicie sesión en CA Enterprise Log Manager como si fuera el usuario Win-Admin y evalúe el acceso que ofrecen las políticas.
6. Si el acceso es demasiado limitado para que el usuario lleve a cabo las tareas necesarias, amplíe el acceso con más políticas.

Paso 1: Creación del usuario Win-Admin

Puede crear un usuario sin función (grupo de aplicaciones) si especifica un acceso a los datos mediante un filtro de acceso.

El primer paso del proceso de restricción del acceso a datos de este modo es la creación del usuario.

Sólo puede crear un usuario si la cuenta de usuarios global no está disponible para su importación desde un directorio externo. Al crear dicha cuenta, no añade detalles del usuario de la aplicación. En este ejemplo, el nombre del usuario es Win-Admin.



Nuevo usuario

Carpeta: _____

Nombre: Win-Admin

Si busca usuarios, el nombre nuevo aparece en la lista.



Más información:

[Creación de un usuario global](#) (en la página 41)

Paso 2: Adición de Win-Admin a la política de acceso a la aplicación de CALM

El segundo paso para restringir el acceso a datos de un usuario llamado Win-Admin es garantizar a esta identidad el acceso a la aplicación de CA Enterprise Log Manager.

Agregue al usuario nuevo a la política de acceso a la aplicación de CALM. El procedimiento es el mismo que el que se realiza al conceder acceso a CA Enterprise Log Manager a una función nueva, salvo que, cuando se buscan identidades, se especifica el tipo como Usuario.

The screenshot shows a configuration window with two tabs: 'General' and 'Identities'.

General Tab:

- Carpeta:** Nombre: CALM Application Access
- Descripción:** This policy defines who all can access the CALM Application
- Calendario:** (empty dropdown)
- Nombre de clase de recursos:** SafeObject
- Tipo:** ☒ Directiva de acceso, ☐ Lista de control de acceso, ☐ Lista de control de identidad de acceso
- Options:** ☐ Rechazo explícito, ☐ Desactivado, ☐ Distribución previa, ☐ Asignar etiquetas

Identities Tab:

Especificar/buscar identidades:

- Tipo:** Usuario
- Atributo:** Nombre de usuario
- Operador:** LIKE
- Valor:** Win-Admin
- Buttons:** Especificar identidades, Win-Admin, Buscar

Identities seleccionadas:

- [Grupo] Administrator
- [Grupo] Analyst
- [Grupo] Auditor
- [Usuario] CALM_API_UT
- [Usuario] Win-Admin

Más información:

[Concesión de acceso a CA Enterprise Log Manager a funciones personalizadas](#)
(en la página 96)

Paso 3: Creación de una política de acceso al sistema de Win-Admin

El paso 2 garantiza el acceso al inicio de sesión en la aplicación de CA Enterprise Log Manager.

El paso 3 restringe o delimita el acceso a la aplicación de CA Enterprise Log Manager tras el inicio de sesión. A grandes rasgos, puede otorgar un acceso de sólo lectura o tanto de lectura como de escritura a las identidades especificadas.

La selección del tipo de política determina la granularidad con la que puede especificar las acciones permitidas.

- Las políticas de acceso permiten realizar acciones seleccionadas en los recursos seleccionados aplicables.
- Las políticas de listas de control de acceso le permiten especificar qué acciones se pueden llevar a cabo en cada recurso añadido.
- Las políticas de listas de control de acceso de identidades le permiten especificar las acciones sobre recursos aplicables que puede llevar a cabo cada identidad.

Puede permitir un acceso limitado a un recurso a través de la creación de un filtro que especifique la carpeta de EEM de dicho recurso e indique las restricciones aplicadas a esa carpeta.

Este ejemplo indica cómo restringir el acceso al acceso de lectura en general con mayores restricciones aplicadas a una función específica. En concreto, el paso 3 restringe al usuario Win-Admin la visualización de los informes de acceso al sistema. El ejemplo siguiente muestra cómo crear una política de ámbito llamada Acceso al sistema de Win-Admin que garantiza el acceso a Objeto seguro y Objeto aplicación, al tiempo que especifica filtros que restringen el acceso a informes a aquellos que cuenten con la etiqueta de acceso al sistema. También indica cómo comprobar la política y, tras la verificación, cómo eliminar la configuración anterior a la implementación.

El área general de una política de ámbito diseñada para especificar el acceso a aplicaciones como de sólo lectura o como de lectura y escritura específica Objeto seguro como nombre de la clase de recurso. En el ejemplo siguiente, se muestra el nombre de la política de Acceso al sistema de Win-Admin. Se recomienda seleccionar una implementación previa para una política nueva hasta que la haya comprobado y esté satisfecho porque esté lista para su uso en un entorno de producción.

Nueva directiva de ámbito [Guardar] [Cerrar]

General

Carpeta:
Nombre: Win-Admin System Access
Descripción:
Calendario:
Nombre de clase de recursos: SafeObject

Tipo:
☒ Directiva de acceso
☐ Lista de control de acceso
☐ Lista de control de identidad de acceso

☐ Rechazo explícito
☐ Desactivado
☒ Distribución previa
☒ Asignar etiquetas

Etiquetas:
Win-Admin

Agregar rótulo: +

Puede otorgar acceso a usuarios o grupos. En este ejemplo, se otorga acceso al nuevo usuario Win-Admin.

Identities

Especificar/buscar identidades
Tipo: Usuario [Buscar identidades]
Identities: [Identities]

Identities seleccionadas
[Usuario] Win-Admin

La política de "mayor nivel" creada para CA Enterprise Log Manager es la política de acceso a CALM, donde CAELM es la instancia de la aplicación. Esta política de ámbito debe especificar que la acción de lectura está permitida en los objetos de la aplicación, AppObject, que hace referencia a todas las funciones de la aplicación.

Configuración de directivas de acceso

Recursos
Agregar recurso:
ApplicationInstance
AppObject

Acciones
read (lectura)
write (escritura)
[Todas las acciones]

Puede limitar más la acción especificada permitida en todos los objetos mediante la definición de filtros. Los filtros se suelen especificar en parejas, donde el primer filtro especifica la carpeta CA EEM en la que se almacenan los datos relacionados con una determinada función y el segundo filtro especifica una restricción sobre los objetos de dicha ubicación. El primer filtro del ejemplo siguiente limita el acceso de la carpeta CA EEM a la carpeta en la que se almacena el recurso de informes. En concreto, especifica que `pozFolder` contiene `/CALM_Configuration/Content/Reports`. El segundo filtro limita el acceso a los informes con la etiqueta de acceso al sistema mediante la especificación de que `calmTag` es igual al acceso al sistema.

Filtros					
Lógica	(	Valor/tipo izquierdo	Operador	Valor/tipo derecho	)
NINGUNO	(	atributo con nombre pozFolder	STRING CONTAINS *..*	valor /CALM_Configuration/	)
Y		atributo con nombre calmTag	STRING EQUAL ==	valor System Access	)

Tras guardar una política, puede realizar una búsqueda de dicha política para revisarla. Puede buscar políticas por nombre, por identidad o por recurso. Puede introducir un valor parcial. También puede introducir múltiples criterios. A continuación, se muestran ejemplos de este caso.

La búsqueda por el nombre completo muestra la única política que busca.

La búsqueda por identidad sólo muestra las políticas que se aplican a esa identidad, incluidas las que se aplican a todas las identidades.

☒ Mostrar directivas coincidentes con la identidad

Identities:

Win-Admin 

Nombre: Win-Admin System Acc

La búsqueda por recurso sólo donde el recurso es AppObject muestra todas las políticas personalizadas y ofrecidas por el sistema que ofrecen acceso de lectura y escritura a una identidad.

Buscar directivas

Concesiones explícitas **Rechazos explícitos**

☐ Mostrar políticas que coincidan con el nombre

☐ Mostrar directivas coincidentes con la identidad

☒ Mostrar directivas coincidentes con el recurso

Nombre de clase de recursos:

SafeObject

Recursos:

AppObject

Cuando la política personalizada que busca aparezca en la tabla de políticas, examine los valores, incluidos los filtros. Si ve que hay algo que se debe corregir, puede hacer clic en el vínculo del nombre para volver a mostrar la política y así poder editarla.

Win-Admin System Access	SafeObject	Concesión explícita	Win-Admin	read	AppObject
Win-Admin Report View POI					

Filtros

WHERE (atributo con nombre: **name:pozFolder** *-* valor: **val:/CALM_Configuration/Content/Reports**

Y atributo con nombre: **name:calmTag** == valor: **val:System Access**)

Esto es muy recomendable para comprobar cada política nueva. Asegúrese de que introduce los pares de atributos/valores en el orden en el que introdujo los filtros, con el atributo de mayor nivel en primer lugar.

Parámetros del control de permisos **Sincronizar caché**

Clase de recurso: SafeObject

Acción: lectura

Recurso: ApplicationInstance

Identidad: Win-Admin

Ejecutar control de permisos

Cuándo:

+ Agregar atributo con nombre

Atributo	Valor	Quitar
pozFolder	/CALM_Configuration/C	
calmTag	System Access	

☒ Incluir directivas de distribución previa con los siguientes rótulos

Rótulos de directivas:

Win-Admin

Agregar rótulo de directiva:

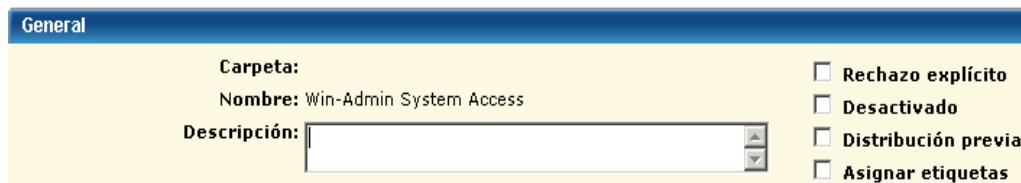
Compruebe que el resultado es ALLOW.

Resultados del control de permisos **Borrar todo**

☐ Mostrar información de depuración ☒ Mostrar obligaciones

Hora del control	Etiquetas de distribución previa	Resultado	Directiva	Delegador	Identidad	Clase de recurso	Recurso	Acción	Cuándo	Atributos con nombre	
										Nombre	Valor
domingo, 27 de septiembre de 2009 18:40:22	Win-Admin	PERMITIR	CALM Application Access		Win-Admin	SafeObject	ApplicationInstance	read		pozFolder	/CALM_Configuration/Content/Reports
										calmTag	System Access

Tras verificar que el resultado es ALLOW, elimine la configuración anterior a la implementación de la política. Si no lo hace, no podrá iniciar sesión como Win-Admin para evaluar las acciones que puede llevar a cabo este usuario.



Más información:

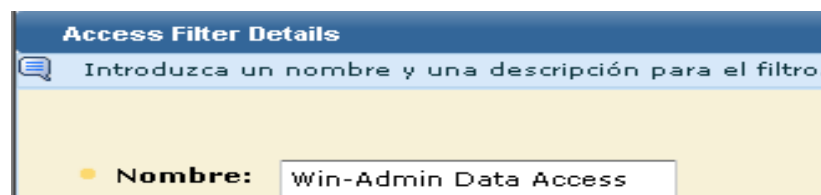
[Comprobación de una política nueva](#) (en la página 108)

Paso 4: Creación de un filtro de acceso a datos de Win-Admin

El paso 3 restringe al usuario Win-Admin la visualización de los informes de acceso al sistema. Este nivel de acceso permite al usuario Win-Admin visualizar los informes de acceso al sistema en las cuatro regiones de la empresa ABC.

El paso 4 crea un filtro de acceso para limitar los datos que puede ver el usuario Win-Admin de los informes de acceso al sistema del controlador del dominio Houston.

La creación de un filtro de acceso a datos comienza por la especificación del nombre. El nombre empleado en este caso es Acceso a datos de Win-Admin.



Especifique las identidades a las que se aplicará el filtro de acceso en el área de identidades. Los filtros pueden aplicarse a usuarios o grupos. En este caso, este filtro de acceso sólo se aplica al usuario Win-Admin.

Para los filtros de acceso, defina cada condición en los valores de una columna de la gramática de eventos comunes. Los valores correspondientes al operador LIKE pueden contener cualquiera de los caracteres comodín siguientes:

- _ (guión bajo): representa un solo carácter
- % (signo de porcentaje): representa una cadena que contiene un número indeterminado de caracteres

El primer filtro, en este caso, aprovecha el hecho de que todos los eventos de Windows cuentan con el prefijo NT-. Para limitar los datos a los eventos de Windows, puede especificar que la columna event_logname de la gramática de eventos comunes deba contener datos que incluyan la cadena NT-%. Para limitar aún más los eventos de Windows a aquellos procedentes de un controlador de dominios determinado, este ejemplo especifica que event_source_hostname debe contener datos que incluyan una cadena que emplee convenciones locales. El valor ABC-HOU-WDC% se basa en una convención de asignación de nombres en forma de nombre con guiones compuesto por las abreviaturas de la empresa, la región y el prefijo del tipo de controlador de dominios.

Filtros avanzados				
Para filtrar los eventos, defina una sentencia condicional en el control de filtros.				
Lógica	(	Columna	Operador	Valor
		event_logname	Como	NT-%
And		event_source_hostname	Como	ABC-HOU-WDC%

Nota: Si no existen orígenes de eventos con una convención de nombres estandarizada, puede crear una lista de valores con clave con los event_source_hostnames que desee y emplear el nombre de la lista de valores con clave como valor.

Cuando sólo hay dos filtros y el operador lógico es AND, no es necesario añadir paréntesis. Si introduce una expresión compleja, como la siguiente, es necesario emplear paréntesis.

```
(event_logname like NT-%
And event_source_hostname=ABC-%)
Or (event_logname like CALM-%
And event_source_hostname=XYZ-%)
```

Al guardar un filtro de acceso a datos, su nombre aparece en la lista de filtros de acceso.



Una búsqueda de políticas coincidentes con el nombre de usuario Win-Admin muestra tres políticas de Todas las identidades y tres más: la política de acceso a la aplicación de CALM, a la que se añadió a Win-Admin; la política de acceso al sistema de Win-Admin creada desde el principio; y la política de datos que se agrega de forma automática cuando define un filtro de acceso. La política de datos se muestra en primer lugar a continuación. También puede verla en las políticas de obligación. Las políticas de obligación nunca se crean directamente mediante CA Enterprise Log Manager.

Directivas de acceso					
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Concesión explícita	ug:Administrator ug:Analyst ug:Auditor Win-Admin	read write	ApplicationInstance AppObject Policy User GlobalUser
49aea1da-caelm54abaf7fc-8876c80-34 Etiquetas: DataPolicy	SafeObligation	Concesión explícita	Win-Admin	FulfillOnGrant	dataaccess/CALM/Data
Win-Admin System Access Etiquetas: Win-Admin	SafeObject	Concesión explícita Distribución previa	Win-Admin	read	AppObject

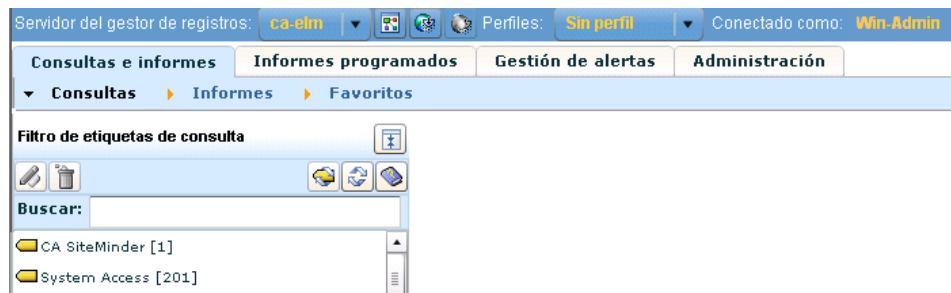
Más información:

[Creación de un filtro de acceso](#) (en la página 111)

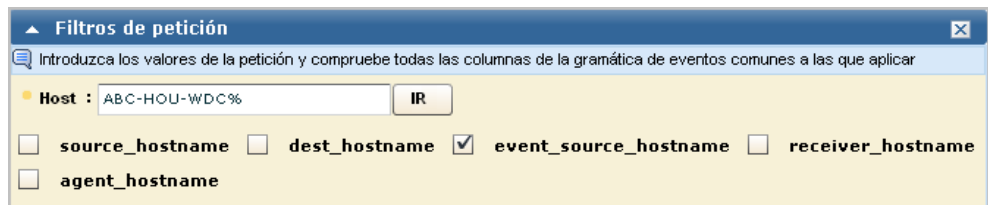
Paso 5: Inicio de sesión como usuario Win-Admin

Al crear políticas para un usuario determinado o un grupo de usuarios de la aplicación, inicie sesión como ese usuario o ese miembro del grupo y determine lo que puede y lo que no puede llevar a cabo. En primer lugar, compruebe que las restricciones esperadas funcionan. En segundo lugar, compruebe que puede llevar a cabo las tareas que espera que puedan realizar estos usuarios.

En este caso, espera poder visualizar sólo los informes o alertas de acción etiquetados como acceso al sistema. En el ejemplo, el único filtro de etiquetas de consultas disponible es el de acceso al sistema. Por lo tanto, se han comprobado las expectativas.



Un método rápido para probar un filtro de acceso es el empleo de la función de peticiones. Sin embargo, esta función no está disponible para el usuario Win-Admin. Todas las consultas de peticiones tienen la etiqueta "Visor de eventos". El acceso a los filtros de peticiones se puede garantizar mediante el filtro de políticas calmTag=Visor de eventos.



El mejor método para comprobar un filtro de acceso es la revisión de los datos visualizados en un informe. Observe el siguiente filtro de acceso. La columna event_logname de la gramática de eventos comunes comienza por NT- y la columna event_source_hostname de la gramática de eventos comunes comienza por ABC-HOU-WDC, la abreviatura de la empresa ABC, la ubicación en Houston y Windows Domain Controller.

```
event_logname Like NT-% AND event_source_hostname Like ABC-HOU-WDC%
```


En el ejemplo siguiente se muestra un informe visualizado por el usuario al que se aplica este filtro de acceso. Tenga en cuenta que los datos de la columna de nombre de registro comienzan por NT- y que los datos de la columna de origen comienzan por ABC-HOU-WDC.

System Access - All Events						
Severidad	Fecha	Origen	Usuario	Acción	Nombre de registro	Categoría
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Información	Jueves, 22/10/09 14:18:22	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management

Paso 6: Ampliación de las acciones permitidas

Las políticas y el filtro de acceso definidos en los pasos 2, 3 y 4 de este ejemplo permiten al usuario Win-Admin visualizar informes de acceso al sistema con límites en los datos mostrados. Sólo con este acceso, el usuario Win-Admin no puede programar un informe, programar una alerta o anotar un informe. Para realizar estas acciones, añada a Win-Admin a la política de acceso al servidor de informes de auditores y analistas y a la política de anotación, programación y creación de analistas. A continuación, se muestra un ejemplo de estas políticas con Win-Admin añadido:

Analyst Auditor Report Server Access Policy Analyst Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	 Concesión explícita	ug:Analyst ug:Auditor Win-Admin	read	AppObject
Analyst Create-Schedule- Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	 Concesión explícita	ug:Analyst Win-Admin	create schedule annotate	Report Alert Tag Profile

Para que Win-Admin pueda crear un informe, este usuario necesita que se añada un acceso de escritura a la política de acceso al sistema de Win-Admin. Esto requiere la apertura de la política de acceso al sistema de Win-Admin para editarla y agregar la escritura a las acciones permitidas.

Win-Admin System Access	SafeObject	 Concesión explícita	Win-Admin	read	AppObject
Win-Admin Report View POI					

Para que Win-Admin pueda emplear peticiones, el filtro del acceso al sistema de Win-Admin puede modificarse de forma que el atributo calmTag equivalga al acceso al sistema o al visor de eventos.

Filtros					
Lógica	(	Valor/tipo izquierdo	Operador	Valor/tipo derecho	)
NINGUNO		atributo con nombre pozFolder	STRING CONTAINS *--*	valor /CALM_Configuration/C	
Y	(	atributo con nombre calmTag	STRING EQUAL ==	valor System Access	
O		atributo con nombre calmTag	STRING EQUAL ==	valor Event Viewer	)

Restricción de acceso a una función: caso de analista de PCI

Puede crear una función parecida a una función predefinida y crear rápidamente políticas basadas en políticas predefinidas. La función definida por el usuario puede parecerse a la función predefinida en que ofrece el mismo acceso a los mismos tipos de recursos, pero se diferencia en que limita el acceso en función de un filtro que no se encuentra en la función predefinida. Puede haber varias políticas a las que se haya agregado esta función predefinida como una identidad. Si la configuración de una política se aplica a la función nueva, sólo debe añadir la función nueva a la política existente. Si la configuración hace que tenga que cambiar el tipo, los recursos, las acciones o los filtros, puede crear una política nueva a partir de una copia de la existente.

Este ejemplo le indica los pasos de la creación de una función para un analista que sólo va a trabajar con informes que tienen una etiqueta de PCI. La política asociada a esta función se crea a partir de una copia de una política existente para todos los analistas.

El proceso consta de los procedimientos siguientes:

1. Planifique las políticas que necesita. En primer lugar, identifique las políticas existentes para aprovecharlas en la función nueva.
2. Cree el nuevo grupo de usuarios (función) de la aplicación, analista de PCI.
3. Ofrezca al analista de PCI un acceso básico a CA Enterprise Log Manager. Agregue esta identidad a la política de acceso a la aplicación de CALM.
4. Ofrezca al analista de PCI un acceso a los servidores de informes y una capacidad de creación de informes igual que la de los analistas. Agregue la identidad del analista de PCI a las políticas identificadas.
5. Restrinja el acceso a informes a aquellos informes con la etiqueta calmTag de PCI. Utilice la política que permita visualizar y editar informes como una plantilla que se puede modificar.
6. Asigne la función de analista de PCI a un usuario de prueba para realizar la evaluación.
7. Inicie sesión como el usuario de prueba y evalúe el acceso.

Si el acceso ofrecido por la función y las políticas es el esperado, asigne la función a todas las personas que deban analizar informes de PCI.

Paso 1: Planificación de la función y de las políticas que se desean crear

Supongamos que desea crear una función parecida a la de los analistas, pero que quiere restringir el acceso a los informes y consultas relacionados con PCI. Planifique un nombre para la función que describa su función, por ejemplo, Analista de PCI.

Antes de comenzar a crear funciones o grupos de usuarios de la aplicación nuevos, tenga en cuenta las políticas que son necesarias para soportar la función nueva. Es aconsejable identificar las políticas existentes que se pueden emplear como plantillas. En las identidades, busque la función que sea similar a la que está planificando.

En este ejemplo, esta función es `ug:Analyst`. En la búsqueda de políticas, seleccione la opción de visualización de las políticas con identidad coincidente, introduzca la identidad, **ug:Analyst**, y haga clic en Ir. Las políticas mostradas incluyen las correspondientes a todas las identidades y las que contienen `ug:Analyst` como identidad.

Directivas de acceso					
Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	 Concesión explícita	ug:Administrator ug:Analyst ug:Auditor	read write	ApplicationInstance AppObject Policy User GlobalUser
Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	 Concesión explícita	ug:Analyst ug:Auditor	read	AppObject
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	 Concesión explícita	ug:Analyst	create schedule annotate	Report Alert Tag Profile
Analyst Report View-Edit Policy Analyst can View/Edit any Report	SafeObject	 Concesión explícita	ug:Analyst	read write	AppObject

Los nombres de políticas que incluyen esta función son las siguientes:

- En el ámbito, la política de acceso a la aplicación de CALM
- En el ámbito, la política de acceso al servidor de informes de auditores y analistas
- En el ámbito, la política de edición y visualización de informes de analistas
- En CALM, la política de creación, programación y anotación de analistas

En cada una de las posibles políticas, examine la definición y determine cuál de las acciones siguientes debe llevar a cabo:

- Adición de la función nueva como identidad a la que se aplica esta política. Esta es la mejor opción si la política se aplica a la función nueva sin ningún cambio.

Esta acción es adecuada para las políticas siguientes del ejemplo:

- Política de acceso a la aplicación de CALM, que define todas las identidades que pueden acceder a CA Enterprise Log Manager.
- Política de acceso al servidor de informes de auditores y analistas, que define todas las entidades que pueden programar informes y alertas en todos los servidores de informes disponibles. Esta función necesita que no haya límites en los servidores de informes.
- Política de creación, programación y anotación de analistas.

- Guarde la política con un nombre nuevo y modifique la definición.

Esta acción es adecuada para la siguiente política de este ejemplo, en la que la copia nueva sólo incluiría la entidad nueva y tendría otro filtro más para limitar el acceso de lectura/escritura a los informes etiquetados como PCI:

- Política de edición y visualización de informes de analistas.

Paso 2: Creación de la función de analista de PCI

Puede crear una función personalizada para representar las tareas que llevan a cabo múltiples usuarios con la aplicación de CA Enterprise Log Manager. Una función es igual que un grupo de usuarios de la aplicación.

El primer paso del proceso de restricción del acceso de una función consiste en la creación de la función.

Al crear una función personalizada que no es un superconjunto de una función existente, no realice una selección desde los grupos de usuarios disponibles.

Nuevo grupo de usuarios de aplicación

General	
Carpeta:	/UserGroups
Nombre:	PCI-Analyst
Descripción:	Role can perform Analyst functions scoped to PCI

Más información:

[Creación de un grupo de usuarios de la aplicación \(función\)](#) (en la página 95)

Paso 3: Adición de analistas de PCI a la política de acceso a la aplicación de CALM

Tras crear una función nueva, el paso siguiente es otorgar a esta función una capacidad de inicio de sesión básica a la aplicación de CA Enterprise Log Manager. De forma predeterminada, sólo las funciones predefinidas tienen acceso al inicio de sesión. Agregue este grupo de aplicaciones a la política de acceso a la aplicación de CALM.

Más información:

[Concesión de acceso a CA Enterprise Log Manager a funciones personalizadas](#) (en la página 96)

Paso 4: Adición de analistas de PCI a políticas existentes

Una vez que haya identificado las políticas que se aplican a un grupo de usuarios de la aplicación cuya función nueva es un subconjunto, debe añadir la función nueva a la lista actual de identidades.

En este caso, añada la función de analista de PCI a las políticas existentes siguientes:

- Política de acceso al servidor de informes de auditores y analistas
- Política de creación, programación y anotación de analistas

Más información:

[Adición de identidades a una política existente](#) (en la página 98)

Paso 5: Creación de políticas basadas en políticas de edición y visualización de informes de analistas

Al crear una política basada en una política existente, debe copiar la política existente y guardarla con un nombre nuevo. A continuación, debe cambiarle el nombre, editar la descripción para que se ajuste a la función nueva y sustituir las identidades existentes por la nueva identidad. Si la política que emplea como plantilla ofrece un acceso demasiado amplio para la función nueva, debe crear filtros para limitar dicho acceso.

En el caso del analista de PCI, debe copiar la política de edición y visualización de informes de analistas, guardarla con otro nombre, abrir la política nueva, sustituir la identidad por la del grupo de analistas de PCI y agregar un filtro para limitar el acceso a informes a aquellos informes que tengan la etiqueta calmTag de PCI.

Filtros

Lógica	(	Valor/tipo izquierdo	Operador	Valor/tipo derecho	)
NINGUNO		atributo con nombre pozFolder	STRING CONTAINS *..*	valor /CALM_Configuration/C	
Y		atributo con nombre calmTag	STRING EQUAL ==	valor PCI	

Es conveniente comprobar una política basada en una política existente como lo haría con una política que hubiese creado desde el principio. Cuando compruebe una política con un filtro, asegúrese de que introduce el filtro del mismo modo en el que se ha introducido en la política. Si introduce un nombre de grupo para la identidad, asegúrese de emplear el prefijo ug:, por ejemplo, ug:analista de PCI.

Parámetros del control de permisos

Clase de recurso: SafeObject
 Acción: escritura
 Recurso: AppObject
 Identidad: ug:PCI-Analyst

Cuándo: Agregar atributo con nombre

Atributo	Valor	Quit
pozFolder	/CALM_Configuration/C	
calmTag	PCI	

Ejecutar control de permisos

Resultados del control de permisos

☒ Mostrar información de depuración ☒ Mostrar obligaciones

Hora del control	Etiquetas de distribución previa	Resultado	Directiva	Delegador	Identidad	Clase de recurso	Recurso	Acción
domingo, 27 de septiembre de 2009 19:45:11		PERMITIR	PCI-Analyst PCI Report View-Edit policy		ug:PCI-Analyst	SafeObject	AppObject	write

Más información:

[Creación de una política basada en una política existente](#) (en la página 106)

[Comprobación de una política nueva](#) (en la página 108)

Paso 6: Asignación de la función de analista de PCI a un usuario

Tras crear una función nueva y sus políticas de soporte, conviene iniciar sesión como un usuario con esa misma función asignada para evaluar si el acceso ofrecido es el adecuado. Una vez que se ha verificado, la función nueva se puede añadir a las cuentas de todos los usuarios que deben llevar a cabo las tareas para las que se ha diseñado la función.

Puede crear una cuenta de usuario temporal con el objetivo de comprobar una función nueva y, a continuación, eliminar la cuenta tras finalizar la comprobación. También puede crear un usuario denominado Usuario de prueba y sustituir la asignación de funciones con cada uso.

Más información:

[Asignación de funciones a usuarios globales](#) (en la página 42)

Paso 7: Inicio de sesión como analista de PCI y evaluación del acceso

Verifique que las políticas son suficientes para limitar el acceso a informes y alertas etiquetados como PCI. Asigne la función de analista de PCI a un usuario e inicie sesión en CA Enterprise Log Manager con los datos de ese usuario.

Visualice las etiquetas de los informes. Compruebe que los informes que puede visualizar son sólo los que tienen la etiqueta de PCI.



Programa un informe. Compruebe que los informes que puede programar son sólo los que tienen la etiqueta de PCI.

Cree un informe. Compruebe que la única etiqueta disponible para el informe nuevo es la de PCI.

Políticas de ejemplo para integraciones personalizadas

Puede ofrecer a los usuarios que no sean administradores la capacidad de crear integraciones personalizadas mediante la creación de una función personalizada, una política de CALM y una política de ámbito. Puede ofrecer a otros usuarios que no sean administradores la capacidad de visualizar integraciones personalizadas mediante la creación de otra función personalizada con una política de ámbito asociada. Añada ambas funciones personalizadas a la política de acceso a la aplicación de CALM y asigne usuarios a dichas funciones.

El procedimiento de ejemplo siguiente indica cómo hacer esto:

1. Cree un grupo de usuarios de la aplicación denominado Crear-archivos-DM-XMP.
2. Cree un grupo de usuarios de la aplicación denominado Visualizar-archivos-DM-XMP.
3. Conceda a Crear-archivos-DM-XMP y a Visualizar-archivos-DM-XMP acceso al producto de CA Enterprise Log Manager.

Nombre/Descripción	Nombre de la clase de recurso	Identities	Acciones	Recursos
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	ug:Administrator ug:Analyst ug:Auditor ug>Create-DM-XMP-Files ug:View-DM-XMP-Files	read write	ApplicationInstance Policy User GlobalUser

4. Cree una política de CALM que ofrezca a Crear-archivos-DM-XMP la capacidad de crear archivos de asignación de datos y archivos de análisis de mensajes mediante la gramática de eventos comunes mientras está conectado a CA Enterprise Log Manager.

Nombre/Descripción	Nombre de la clase de recurso	Identities	Acciones	Recursos
Integration-Create policy Can create data mapping and message parsing files using common event grammar.	CALM	ug>Create-DM-XMP-Files	create	Integration

5. Cree una política de ámbito que ofrezca a Crear-archivos-DM-XMP la capacidad de editar y visualizar los archivos de asignación de datos personalizados y el archivo XMP guardados en la carpeta de EEM /CALM_Configuration/Content/Mapping o /CALM_Configuration/Content/Parsing mediante la gramática de eventos comunes.

Nombre/Descripción	Nombre de la clase de recurso	Identities	Acciones	Recursos
Edit-DM-XMP-Files with CEG Policy Can edit data mapping files and message parsing files using common event grammar saved to the EEM folders /CALM_Configuration/Content/...	SafeObject	ug>Create-DM-XMP-Files	read write	AppObject

Filtros	
WHERE	name:pozFolder *--* val:/CALM_Configuration/Content/Mapping
O	name:pozFolder *--* val:/CALM_Configuration/Content/Parsing

6. Cree una política de ámbito que ofrezca a Visualizar-archivos-DM-XMP la capacidad de visualizar los archivos de asignación de datos personalizados y el archivo XMP guardados en la carpeta de EEM
/CALM_Configuration/Content/Mapping o
/CALM_Configuration/Content/Parsing.

Nota: La política de la gramática de eventos comunes otorga a todas las identidades el derecho a visualizar la gramática de eventos comunes.

Nombre/Descripción	Nombre de la clase de recurso	Identidades	Acciones	Recursos
View-DM-XMP-Files Can view data mapping files and message parsing files.	SafeObject	ug:View-DM-XMP-Files	read	AppObject

Filtros	
WHERE	(name:pozFolder *--* val:/CALM_Configuration/Content/Mapping
O	name:pozFolder *--* val:/CALM_Configuration/Content/Parsing)

7. Compruebe las políticas.
8. Asigne usuarios tanto a Crear-archivos-DM-XMP como a Visualizar-archivos-DM-XMP.

Políticas de ejemplo para reglas de supresión y resumen

Puede autorizar a usuarios que no sean administradores a crear reglas de supresión personalizadas y reglas de resumen personalizadas mediante la creación de una función personalizada, una política de CALM y una política de ámbito. Puede ofrecer a otros usuarios que no sean administradores la capacidad de visualizar reglas de supresión personalizadas y reglas de resumen personalizadas mediante la creación de otra función personalizada con una política de ámbito asociada. Añada ambas funciones personalizadas a la política de acceso a la aplicación de CALM y asigne usuarios a dichas funciones.

El procedimiento de ejemplo siguiente indica cómo hacer esto:

1. Cree un grupo de usuarios de la aplicación denominado Crear-reglas-SUP-SUM.
2. Cree un grupos de usuarios de la aplicación denominado Visualizar-reglas-SUP-SUM.
3. Conceda a ambas funciones acceso al producto de CA Enterprise Log Manager.

Nombre/Descripción	Nombre de la clase de recurso	Identities	Acciones	Recursos
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	ug:Administrator ug:Analyst ug:Auditor ug:Create-Sup-Sum-Rules ug:View-Sup-Sum-Rules	read write	ApplicationInstance Policy User GlobalUser

4. Cree una política de CALM que conceda a los usuarios de Crear-reglas-SUP-SUM la capacidad de crear reglas de resumen y supresión o importarlas mientras están conectados a CA Enterprise Log Manager.

Nombre/Descripción	Nombre de la clase de recurso	Opciones	Identities	Acciones	Recursos
EventGroup-Create policy Can create custom summarization and suppressionrules or import rules.	CALM	 Concesión explícita	ug:Create-Sup-Sum-Rules	create	EventGrouping

5. Cree una política de ámbito que ofrezca a los usuarios de Crear-reglas-SUP-SUM la capacidad de visualizar o editar reglas de resumen o supresión personalizadas almacenadas en la carpeta de EEM, /CALM_Configuration/Content/Rules/Suppression o /CALM_Configuration/Content/Rules/Summarization.

Nombre/Descripción	Nombre de la clase de recurso	Identities	Acciones	Recursos
View-Edit-SUP-SUM-Rules Can view or edit suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	ug:Create-Sup-Sum-Rules	read write	AppObject

Filtros				
WHERE	name:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Summarization	
O	val:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Suppression	

6. Cree una política de ámbito que ofrezca a los usuarios de Visualizar-reglas-SUP-SUM la posibilidad de visualizar reglas de resumen o de supresión personalizadas.

Nombre/Descripción	Nombre de la clase de recurso	Identities	Acciones	Recursos
View-SUP-SUM-Rules Can view suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	ug:View-Sup-Sum-Rules	read	AppObject

Filtros				
WHERE	name:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Summarization	
O	val:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Suppression	

7. Compruebe las políticas.
8. Asigne usuarios a las funciones nuevas. Por ejemplo, es posible que haya auditores externos que deseen visualizar las reglas de resumen y supresión. Para permitirlo, puede asignar una función similar a Ver-reglas-Sup-Sum a dichos usuarios.

Otra opción, en lugar de crear dos funciones nuevas especialmente para la tarea de creación/edición/visualización y la tarea de sólo visualización, es la ampliación de las funciones predefinidas Analyst y Auditor. Por ejemplo, puede eliminar los pasos 1, 2, 3 y 8 del procedimiento anterior y, en su lugar, asignar Analyst como identidad a la política Crear-EventGrouping y Visualizar-reglas-Edit-SUP-SUM, y asignar Auditor del grupo de usuarios como identidad en Visualizar-reglas-SUM-SUP.

Más información:

[Creación de un grupo de usuarios de la aplicación \(función\)](#) (en la página 95)

[Concesión de acceso a CA Enterprise Log Manager a funciones personalizadas](#)
(en la página 96)

[Comprobación de una política nueva](#) (en la página 108)

[Asignación de funciones a usuarios globales](#) (en la página 42)

Capítulo 5: Servicios y adaptadores de CA

Esta sección contiene los siguientes temas:

[Tareas de servicios](#) (en la página 152)

[Eliminación de hosts de servicio](#) (en la página 153)

[Edición de configuraciones globales](#) (en la página 154)

[Edición de configuraciones del servicio global](#) (en la página 157)

[Edición de configuraciones del servicio local](#) (en la página 158)

[Configuraciones de servicio](#) (en la página 159)

[Tareas de configuración de adaptadores de CA](#) (en la página 182)

[Tareas de estado del sistema](#) (en la página 189)

Tareas de servicios

Puede establecer configuraciones globales que se apliquen a todos los servidores de CA Enterprise Log Manager. Puede ver y editar dos tipos de configuraciones de servicio individuales: una configuración de servicio global se aplica a todas las instancias de un único servicio en su entorno, y una configuración de servicio local sólo se aplica a un determinado host de servicio individual.

Nota: Las configuraciones globales son distintas de las configuraciones de *servicio* globales: la primera controla el comportamiento de todos los servidores de CA Enterprise Log Manager, mientras que la segunda controla el del servicio seleccionado. Por ejemplo, puede establecer el intervalo de actualización para todos los servicios (configuración global), o políticas de retención de informes para todos los servidores de informes (configuración de servicio global).

También puede visualizar eventos autocontrolados desde las áreas de configuración de servicio.

Los servicios disponibles incluyen:

- Gestor de agentes
- Servicio de alertas
- Servicio de correlación
- Almacenamiento de registro de eventos
- Servicio del incidente
- Servidor de ODBC
- Consulta de servicio
- Servidor de informes
- Servicio de prueba de reglas
- Servicio de suscripción
- Estado del sistema

Puede visualizar algunos servicios por nombre de servicio o por host. Puede utilizar el servicio de estado del sistema para recopilar información relativa a un servidor individual de CA Enterprise Log Manager y controlar dicho servidor.

Más información:

[Edición de configuraciones del servicio global](#) (en la página 157)

[Edición de configuraciones del servicio local](#) (en la página 158)

Eliminación de hosts de servicio

Si desinstala un servidor de CA Enterprise Log Manager, debe eliminar la configuración del host del repositorio del servidor de gestión. La eliminación de esta referencia permitirá que el servidor se mantenga actualizado con la lista de sus servidores de CA Enterprise Log Manager registrados.

Para eliminar hosts de servicio

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
Aparece la lista de servicios.
2. Haga clic en Host en el cuadro de diálogo Mostrar servicios por situado en la parte superior de la lista.
Aparece una lista de árbol ampliable con los hosts de servicio.
3. Seleccione el host que desea suprimir y, a continuación, haga clic en Suprimir.
El host se elimina de la lista.

Importante: Al eliminar hosts, no se muestran advertencias. Al hacer clic en Suprimir, el host se elimina de forma inmediata, así que debe estar seguro de que desea eliminar el host.

Edición de configuraciones globales

Puede definir configuraciones globales para todos los servicios. Si intenta guardar valores que se encuentran fuera del intervalo permitido, CA Enterprise Log Manager adoptará de forma predeterminada al valor mínimo o máximo, según corresponda. Algunos de los ajustes son interdependientes.

Para editar configuraciones globales

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.

Aparece la lista de servicios.

2. Haga clic en Configuración global en la lista de servicios.

Se abre el panel de detalles de la configuración del servicio global.

3. Cambie cualquier de los ajustes de configuración siguientes:

Intervalo de actualización

Especifica la frecuencia, en segundos, con la que los componentes del servidor aplican actualizaciones de configuración.

Mínimo: 30

Máximo: 86400

Tiempo de espera de sesión

Especifica la duración máxima de una sesión inactiva. Si se activa la actualización automática, la sesión nunca caduca.

Mínimo: 10

Máximo: 600

Permitir actualización automática

Permite a los usuarios actualizar los informes y las consultas de forma automática. Este valor permite a los administradores desactivar la actualización automática de forma global.

Frecuencia de la actualización automática

Especifica el intervalo (en minutos) en el que se actualiza la visualización del informe. Este valor depende de la selección de Permitir actualización automática.

Mínimo: 1

Máximo: 60

Permitir actualización automática

Establece la actualización automática en todas las sesiones. De forma predeterminada, la actualización automática no está activada.

La visualización de las alertas de acción requiere autenticación

Evita que los auditores o los productos de terceros vean las fuentes RSS de las alertas de acción. Este ajuste está activado de forma predeterminada.

Informe predeterminado

Especifica el informe predeterminado.

Activar inicio de informe predeterminado

Muestra el informe predeterminado al hacer clic en la subficha Informes. Este ajuste está activado de forma predeterminada.

4. Cambie cualesquiera de los valores de etiquetas de informe y consulta siguientes:

Ocultar etiquetas de informe

Evita que las etiquetas especificadas aparezcan en una lista de etiquetas. Al ocultar las etiquetas de informe se simplifica la visión de los informes disponibles.

Ocultar etiquetas de consulta

Permite ocultar las etiquetas seleccionadas. Las etiquetas ocultas no aparecen en la lista de consultas principal ni en la lista de consultas sobre la programación de alertas de acción. Al ocultar las etiquetas de consulta se personaliza la vista de las consultas disponibles.

5. Cambie cualesquiera de las siguientes configuraciones del cuadro de mandos:

Activar inicio del cuadro de mandos predeterminado

Muestra el cuadro de mandos predeterminado al hacer en las fichas Consultas e Informes. Este ajuste está activado de forma predeterminada.

Cuadro de mandos predeterminado

6. Cambie cualesquiera de los ajustes de perfil siguientes:

Activar perfil predeterminado

Permite definir el perfil predeterminado.

Perfil predeterminado

Especifica el perfil predeterminado.

Ocultar perfiles

Permite ocultar los perfiles seleccionados. Cuando la interfaz se actualiza o caduca el intervalo de actualización, los perfiles ocultos no aparecen. Al ocultar los perfiles se personaliza la vista de los perfiles disponibles.

Nota: Haga clic en Restablecer para restaurar los últimos valores guardados. Hasta que guarde los cambios, puede restablecer un solo cambio o varios. Una vez que haya guardado los cambios, deberá restablecerlos de forma individual.

7. Haga clic en Guardar.

Edición de configuraciones del servicio global

Puede editar configuraciones del servicio global, que son configuraciones que se aplican a instancias de un determinado servicio en su entorno. Las configuraciones del servicio global *no* anulan las configuraciones del servicio local que no coincidan con la configuración global.

Los valores de configuración máximos y mínimos se detallan en las secciones de servicio específicas. Si intenta guardar valores que se encuentran fuera del intervalo permitido, CA Enterprise Log Manager adoptará de forma predeterminada al valor mínimo o máximo, según corresponda.

Para editar configuraciones del servicio global

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.

Aparece la lista de servicios.

2. Seleccione el servicio cuya configuración desee editar.

Se abre la pantalla Configuración del servicio global en el panel de detalles.

3. Introduzca los cambios de configuración que desee.

Nota: Puede hacer clic en Restablecer para restablecer los campos de entrada al último valor guardado. Puede restablecer un único cambio o varios cambios hasta el momento en que haga clic en Guardar. Una vez que haya guardado los cambios, deberá restablecerlos de forma individual.

4. Cuando haya terminado de introducir cambios, haga clic en Guardar.

Los cambios de configuración se aplicarán a todos los hosts del servicio seleccionado, a no ser que tengan configuraciones locales diferentes.

Edición de configuraciones del servicio local

Puede ver o editar las configuraciones de servicio local por servicio o por servidor de host. Las configuraciones de servicio local le permiten controlar los servicios o las configuraciones que podrían no aplicarse, o ser necesarias, para todo el entorno, anulando la configuración local sólo en el caso de hosts específicos. Por ejemplo, puede que desee que un servidor de CA Enterprise Log Manager determinado retenga alertas de acción durante más tiempo que los demás. Esto lo puede controlar mediante la configuración local.

Los valores de configuración máximos y mínimos se detallan en las secciones de servicio específicas. Si intenta guardar valores que se encuentran fuera del intervalo permitido, CA Enterprise Log Manager adoptará de forma predeterminada al valor mínimo o máximo, según corresponda.

Para editar configuraciones del servicio local

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.

Aparece la lista de servicios.

2. Haga clic en la flecha situada junto al servicio cuya configuración desea editar.

La pantalla del servicio se amplía y muestra los hosts de servicio individuales.

3. Haga clic en el host de servicio que desea.

Se abre la configuración del servicio seleccionada en el panel de detalles.

4. Introduzca los cambios de configuración que desee. Todos los campos de entrada, menús o controles de la configuración local cuentan con un botón de configuración local/global que se puede establecer en uno de los dos estados.

Configuración global: 

Configuración local: 

Un clic en el botón modifica la configuración de global a local y hace que el valor asociado esté disponible para su uso. El valor debe permanecer establecido en la configuración local para que el ajuste tenga efecto: si se establece en la configuración global, se aplicará la configuración global de esa escucha.

Nota: Al hacer clic en Restablecer, se muestran los valores de configuración almacenados más recientemente para las configuraciones disponibles. Puede restablecer un único cambio o varios cambios hasta el momento en que haga clic en Guardar. Una vez que haya guardado los cambios, deberá restablecerlos de forma individual.

5. Cuando haya terminado de introducir cambios, haga clic en Guardar.
Los cambios que realice sólo se aplicarán al host de servicio seleccionado.

Configuraciones de servicio

En esta sección se incluyen detalles y directrices de servicio que se deben tener en cuenta al realizar cambios en la configuración de los servicios de CA Enterprise Log Manager siguientes:

- Servicio de alertas: controla la configuración de entrega para las alertas de acción, incluidas las configuraciones de los servidores SMTP, de CA IT PAM y de los mensajes SNMP.
- Servicio de correlación: controla las reglas de correlación de controles y el enrutamiento de eventos para la creación de incidentes.
- Almacenamiento de registro de eventos: almacena todos los eventos sin formato refinados y registrados.
- Servicio del incidente: controla la creación y el almacenamiento de incidentes que resultan de la correlación de eventos.
- Servidor ODBC: permite acceder al almacén de registro de eventos de CA Enterprise Log Manager desde una aplicación externa como, por ejemplo, Informes de BusinessObjects Crystal.
- Servidor de informes: controla la distribución, el formato y la retención de informes y alertas.
- Servicio de suscripción: enruta actualizaciones del contenido y la configuración al servidor de gestión, y actualizaciones binarias a los clientes de la suscripción.

Más información:

[Suscripción](#) (en la página 235)

Consideraciones del servicio de alertas

El servicio de alertas controla la entrega de alertas de acción. En el área de configuración del servicio de alertas, puede realizar las siguientes tareas:

- Establecer el servidor de correo, el correo electrónico de admin, así como la información del puerto SMTP y de autenticación para la entrega de alertas en el área Configuración del correo electrónico.
- Configurar la integración con IT PAM para alertas de acción.
- Configurar la integración de ObserveIT.
- Configurar mensajes SNMP para la entrega de alertas de acción.

Más información:

[Configuración de CA Enterprise Log Manager para funcionar con ObserveIT](#) (en la página 164)

[Configuración de la integración con un destino de trap de SNMP](#) (en la página 166)

Configuración de la integración de CA IT PAM

La integración de CA IT PAM se puede configurar para optimizar uno de los tipos siguientes de procesos de CA IT PAM o ambos:

- Proceso de salida de alerta/evento: un proceso que invoca el procesamiento de un sistema de terceros.
- Proceso de valores dinámicos: un proceso que acepta una clave de entrada y devuelve valores actuales para esa clave como un archivo de valores separados por comas (*.csv).

El procedimiento siguiente dirige los dos valores de configuración comunes.

Para configurar la integración de CA IT PAM

1. Haga clic en la ficha Administración y en la subficha Servicios.
2. Haga clic en servicio de alertas.

Aparecerá el cuadro de diálogo Configuración del servicio global: Servicio de alertas.

3. Desplácese al área de CA IT PAM.
4. Introduzca el nombre de host completo del servidor en el que esté instalado CA IT PAM, acepte el número de puerto predeterminado, 8080, y especifique las credenciales válidas de inicio de sesión para CA IT PAM.
5. Realice las acciones siguientes para el proceso de salida de alerta/evento de la sección Proceso de salida de alerta/evento:

- a. Si ha importado el ejemplo EventAlertOutput.xml para utilizarlo, acepte la entrada predeterminada para el proceso de salida de alerta/evento. Si no es así, sustituya esta entrada por el nombre de su proceso de salida de alerta/evento personalizado precedido por esta ruta.

Nota: En Carpetas, en el cliente de ITPAM, puede ver el nombre y la ruta del proceso.

- b. Si ha importado el ejemplo EventAlertOutput.xml para utilizarlo, defina los valores predeterminados para NotificadoPor, Severidad, Prioridad y UsuarioFinal como se indica a continuación:

- a. Seleccione un parámetro y haga clic en Agregar valor predeterminado.

Aparecerá el cuadro de diálogo Agregar valor.

- b. Introduzca el valor predeterminado y haga clic en Aceptar.

- c. Si especificó un proceso de salida de alerta/evento personalizado, suprima los parámetros que se muestran y agregue los que desee. A continuación, defina el valor predeterminado para cada uno.

6. Realice las acciones siguientes para la actualización programada de la lista de claves en la sección Actualización de la lista de claves:

- a. Seleccione el servidor que actualiza la lista de claves de la lista de servidores predeterminados.

- b. Seleccione la opción Activado.

Se muestran los parámetros necesarios para la programación.

- c. Seleccione la zona horaria y la hora de inicio a las cuales se ejecuta el programador de la actualización.

- d. Seleccione la frecuencia de repetición del programador de la actualización y especifique los detalles requeridos.

7. Haga clic en Guardar.

Aparecerá el mensaje siguiente: Confirmación: Los cambios en la configuración se han guardado correctamente. La integración de CA IT PAM se ha configurado.

Más información:

[Creación de una lista con claves](#) (en la página 356)

Integración de ObserveIT

Se puede integrar CA Enterprise Log Manager con ObserveIT para consultar las grabaciones de las sesiones de usuario.

Con ObserveIT pueden realizarse las actividades siguientes:

- Control de las actividades de configuración de todos los usuarios
- Control de todas las actividades de usuario sospechosas
- Generación de informes en todas las actividades de usuario

Se pueden utilizar una o varias instancias de ObserveIT.

Nota: Para obtener más información acerca del control de las actividades de los usuarios, consulte la documentación de ObserveIT.

Más información:

[Consideraciones de la integración](#) (en la página 163)

[Configuración de CA Enterprise Log Manager para funcionar con ObserveIT](#) (en la página 164)

[Consulta de una grabación de una sesión de usuario](#) (en la página 165)

Modo de integración de CA Enterprise Log Manager con ObserveIT

A continuación se proporciona una descripción general de los pasos que debe realizar el administrador para integrar CA Enterprise Log Manager con ObserveIT.

Para integrar CA Enterprise Log Manager con eTrust Audit, realice los pasos siguientes:

- Configure CA Enterprise Log Manager para trabajar con ObserveIT.
- Consulte una grabación de una sesión de usuario.

Consideraciones de la integración

CA Enterprise Log Manager admite la integración con ObserveIT 5.2.5.1. Antes de integrar CA Enterprise Log Manager con ObserveIT, realice las acciones siguientes:

- Verifique que se ha instalado el servidor ObserveIT.
- Si desea consultar las grabaciones de las sesiones de usuario desde varias instancias de ObserveIT, verifique que ha instalado el servidor de gestión centralizado de ObserveIT.
- Si desea recopilar registros de ObserveIT desde un origen del evento, verifique que ha implementado un conector de ObserveIT para cada base de datos de ObserveIT en el origen del evento. Para obtener más información acerca del conector de ObserveIT, consulte la *Guía del conector para ObserveIT*.

Nota: Para obtener más información acerca de la instalación de ObserveIT, consulte la documentación de ObserveIT.

Configuración de CA Enterprise Log Manager para funcionar con ObserveIT

El funcionamiento conjunto de CA Enterprise Log Manager con ObserveIT permite consultar grabaciones de sesiones de usuario. Para integrar CA Enterprise Log Manager con ObserveIT, debe configurarse el servidor ObserveIT desde la interfaz de CA Enterprise Log Manager.

Para configurar CA Enterprise Log Manager para funcionar con ObserveIT

1. Haga Clic en Administración, Servicios y Servicio de alerta.

Aparecerá la ventana Configuración global del servicio: Servicio de alerta. Se abre la ficha Administración de forma predeterminada.

Nota: Se puede configurar un servidor de CA Enterprise Log Manager individual para funcionar con ObserveIT a nivel de configuración regional.

2. Complete los campos siguientes en el panel ObserveIT según sea necesario y haga clic en Guardar:

URL del servidor ObserveIT

Especifica la dirección del servidor ObserveIT.

Nota: Si se utiliza una sola instancia de ObserveIT, debe especificarse la dirección del servidor ObserveIT en el formato siguiente:

`http://observeit_appserver:port_number_used_to_install_ObserveIT/ObserveIT`

Si se utilizan varias instancias de ObserveIT, debe especificarse la dirección del servidor de gestión centralizado en el formato siguiente:

`http://observeit_centralizedmanagementserver/ObserveITCentralizedManagement/`

Nombre de usuario

Especifica el nombre de usuario del administrador con acceso al servidor ObserveIT.

Contraseña

Especifica la contraseña asociada al administrador del servidor ObserveIT.

3. (Opcional) Haga clic en Conexión de prueba.

Se prueba la conexión al servidor ObserveIT. Si la conexión se realiza correctamente, se muestra el mensaje La información de la conexión con ObserveIT se ha validado correctamente. El servidor de aplicaciones de ObserveIT se configura desde el servidor de CA Enterprise Log Manager.

Más información:

[Consideraciones de la integración](#) (en la página 163)

[Consulta de una grabación de una sesión de usuario](#) (en la página 165)

Consulta de una grabación de una sesión de usuario

CA Enterprise Log Manager permite consultar una sesión de usuario grabada por ObserveIT. Para consultar una grabación de una sesión de usuario, el usuario debe tener el rol de administrador o analista. Se puede consultar una grabación de sesión de usuario cuando se inicia el visor de consultas mediante la API de CA Enterprise Log Manager.

Para consultar una grabación de una sesión de usuario

1. Haga clic con el botón secundario del ratón en un evento de un informe y seleccione Buscar host por grabación de sesión de usuario.

Se abrirá el cuadro de diálogo Eventos de grabación de sesiones de usuario de ObserveIT. El cuadro de diálogo muestra todas las grabaciones de las sesiones de usuario disponibles dentro del período de tiempo del evento seleccionado y de la hora actual.

2. Haga clic en el icono de vídeo de la sesión que desee consultar.

Nota: El icono de vídeo solamente se activa si hay un evento dentro del período de tiempo seleccionado.

Se abrirá la ventana del visualizador de diapositivas de ObserveIT. Se reproduce la grabación de la sesión de usuario seleccionada.

Más información:

[Consideraciones de la integración](#) (en la página 163)

[Configuración de CA Enterprise Log Manager para funcionar con ObserveIT](#) (en la página 164)

Configuración de la integración con un destino de trap de SNMP

Configure la integración de SNMP como parte de la configuración del servicio global para el servidor de informes. La configuración es la dirección IP y el puerto de un destino de trap de SNMP.

La integración de SNMP se puede configurar antes o después de preparar el producto de destino para que reciba e interprete traps de SNMP desde CA Enterprise Log Manager.

Cuando cree una alerta destinada a un destinatario de trap de SNMP, puede especificar uno o más destinos. Esta configuración sirve como el valor predeterminado. Este valor predeterminado se aplica a todos los servidores incluidos en el servidor de informes.

Para configurar la integración de SNMP

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Haga clic en Servicio de alertas.
Aparecerá el cuadro de diálogo Configuración del servicio global: Servicio de alertas.
3. Desplácese hasta el área Configuración de SNMP.
4. Introduzca la dirección IP o el nombre de host del servidor de destino para traps de SNMP.
5. Acepte el puerto predeterminado 162 o modifíquelo.
6. Haga clic en Guardar.

Consideraciones del servicio de correlación

El servicio de correlación controla las reglas aplicadas en el servidor de correlación. Una regla se activa cuando se aplica.

Es posible asociar destinos de notificación con reglas y activar o desactivar las reglas desde la página de configuración del servicio de correlación. Es posible elegir qué servidores de CA Enterprise Log Manager enrutan eventos al servidor de correlación seleccionado o bien establecer un límite del evento.

Límite del evento

Define la cantidad de eventos que se retendrán por incidente cuando se permita la acumulación. El límite de eventos ayuda a evitar el tráfico indebido causado por la correlación en períodos de elevada actividad. Cuando se alcanza este límite, los eventos adicionales se pierden. Por ejemplo, si se establece un límite de 100, cada regla puede acumular hasta 100 eventos registrados, entre los cuales se incluyen los eventos, o evento, iniciales que cumplen los requisitos. La acumulación continúa hasta que se alcanza el límite de eventos o, lo que es más habitual: hasta que los valores de intervalo o límite restablecen la regla.

También se pueden eliminar reglas de correlación aplicadas, con lo cual éstas quedan inactivas.

Para eliminar reglas de la lista aplicada

1. Resalte la fila de la regla de correlación que desee eliminar.
2. (Opcional) Puede hacer clic mientras mantiene pulsada la tecla Ctrl o la tecla de mayúsculas para resaltar varias filas.
3. Haga clic en Eliminar.

Las reglas resaltadas se eliminan de la lista activa.

4. Haga clic en Guardar para confirmar la configuración. Si no ha guardado, puede hacer clic en Restablecer para restaurar reglas eliminadas de la lista.

Nota: Este procedimiento solamente elimina reglas de correlación de la lista activa. No se eliminan reglas de la biblioteca de reglas.

Consideraciones del almacén de registro de eventos

El almacenamiento de registro de eventos emplea un sistema federado de almacenamiento de registro de eventos, en el que cada servidor de host mantiene su almacenamiento de registro de eventos local y tiene la posibilidad de ponerse en contacto con otros almacenamientos de registro de eventos de su entorno. Cuando envía una consulta a un servidor para obtener información sobre eventos, puede buscar en su propio sistema de almacenamiento de registro de eventos, así como en todos los demás sistemas conectados mediante la federación. Esta disposición permite un almacenamiento y un archivo flexibles de los datos de eventos.

La configuración de archivo del almacenamiento de registro de eventos permite especificar la frecuencia con la que se almacenan los datos y su ubicación. Se envían consultas para obtener información tanto de almacenamientos de registro de eventos calientes (activos) como tibios (archivados). La información de eventos en almacenamiento frío (remoto) no se solicita.

Puede configurar los siguientes ajustes de archivo y de almacenamiento de registro de eventos:

Número máximo de filas

Establece el número máximo de eventos que puede contener la base de datos caliente de almacenamiento de registro de eventos. Cuando el recuento de eventos alcanza este valor, el registro de eventos comprime toda la información de eventos en la base de datos caliente y los traslada a la base de datos tibia.

Mínimo: 50000

Máximo: 100000000

Número máximo de días de archivado

Establece el número días que se retienen los archivos almacenados en el archivo antes de eliminarlos.

Mínimo: 1

Máximo: 28000

Archivar espacio en disco

Define el porcentaje de espacio en disco disponible que activa la eliminación automática de los archivos de almacenamiento más antiguos. Por ejemplo, el valor predeterminado es 10. Cuando el espacio disponible del sistema de almacenamiento de registro de eventos está por debajo del 5%, el registro de eventos elimina los archivos más antiguos para ampliar el espacio.

Mínimo: 10

Máximo: 90

Política de exportación

Define el número de horas durante las que un archivo restaurado de un origen de copia de seguridad externo del archivo (descongelado) se retendrá en el sistema de almacenamiento de registro de eventos antes de eliminarse.

Mínimo: 0

Máximo: 168

Reglas de resumen/supresión

Controla cuál de las reglas de resumen o supresión se aplica a los eventos recibidos. Las reglas de resumen o supresión nuevas debe aplicarlas un administrador antes de que comiencen a refinar eventos.

Reglas de transferencia

Controla cuál de las reglas de transferencia de eventos se aplica a los eventos recibidos.

Secundarios de la federación

Controla cuáles de los sistemas de almacenamiento de registro de eventos disponibles se definen como secundarios del servidor actual. Esto le permite establecer "árboles" de federación independientes que controlan los niveles de acceso a las consultas. Este valor sólo está disponible como configuración local.

La configuración de registro controla el modo en que los módulos de CA Enterprise Log Manager individuales registran los mensajes internos. Sólo está disponible como configuración local. La configuración de registro se suele emplear para solucionar problemas. Normalmente, no hay que modificar esta configuración y sólo tendrá que conocer bien el registro y los archivos de registro antes de realizar modificaciones.

Nivel de registro

Define el tipo y el nivel de detalle incluidos en el archivo de registro. La lista desplegable se ordena según el detalle, donde la primera opción ofrece la información menos detallada, y la última ofrece la más detallada.

Aplicar a todos los registradores

Controla si la configuración del nivel de registro anula todos los ajustes de registro del archivo de propiedades de registro. Este ajuste sólo se aplica cuando la configuración del nivel de registro es inferior (muestra más detalles) a la configuración predeterminada.

La configuración de archivo automático activa y controla las tareas programadas de archivo de la base de datos, lo que desplaza las bases de datos tibias a un servidor remoto.

Nota: Antes de mover tareas de base de datos programadas de un servidor de CA Enterprise Log Manager a otro o a un servidor remoto, debe configurar la autenticación no interactiva entre los servidores. Consulte la sección de Configuración de autenticación no interactiva de la *Guía de implementación de CA Enterprise Log Manager* para obtener más información.

Puede establecer los siguientes valores de archivo automático:

Activado

Establece la ejecución de una tarea de archivo automático. El archivo automático emplea la utilidad scp tal y como la controlan otros ajustes.

Tipo de copia de seguridad

Controla el tipo de copia de seguridad: archivo completo que copia toda la información de la base de datos, o archivo incremental que copia todas las bases de datos que aún no se han guardado en la copia de seguridad.

Valor predeterminado: Incremental

Frecuencia

Especifica si la tarea de archivo se ejecuta cada día o cada hora. Una tarea diaria se ejecuta en el momento establecido mediante el reloj de hora de inicio. Una tarea ejecutada cada hora se lleva a cabo cada hora en punto.

Hora de inicio

Establece la hora en que se ejecuta una tarea de archivo diaria, en horas completas, según la hora local del servidor. El valor corresponde a un reloj de 24 horas.

Límites: 0-23, donde 0 equivale a la medianoche y 23 equivale a las 11.00 p.m.

Usuario de EEM

Especifica el usuario que puede llevar a cabo una consulta de archivo, recatalogar la base de datos, ejecutar la utilidad LMArchive y ejecutar el script shell restore-ca-elm con el fin de restaurar bases de datos de archivo para su examen. A este usuario se le debe asignar la función predeterminada de administrador o una función personalizada asociada a una política personalizada que permita la acción de edición en un recurso de la base de datos.

Valor predeterminado: usuario del administrador del gestor de registros

Contraseña de EEM

Especifica la contraseña del usuario que tiene los derechos definidos en el campo de usuario de EEM.

Servidor remoto

Especifica el nombre del host o la dirección IP del servidor remoto al que la tarea de archivo automático copia la información de la base de datos.

Usuario remoto

Especifica el nombre de usuario que emplea la utilidad scp para conectarse al servidor remoto.

Valor predeterminado: caelmservice

Ubicación remota

Especifica el destino del archivo de almacenamiento en el servidor remoto.

Valor predeterminado: /opt/CA/LogManager

Servidor de ELM remoto

Especifica si el servidor remoto es un servidor de gestión o no. Si lo es, entonces la tarea de archivo automático eliminará las bases de datos del equipo local cuando la transferencia haya finalizado y notificará al equipo remoto para que realice una recatalogación.

Período de recepción de eventos de correlación

Controla la variación de tiempo máxima tolerada para la creación de incidentes. Los dos valores permiten establecer un valor después del tiempo de servidor de CA Enterprise Log Manager actual (futuro) y antes del tiempo de servidor de CA Enterprise Log Manager actual (pasado). Si un evento se queda fuera de ese intervalo no se transmite para la correlación.

Más información:

[Almacenamiento de registros](#) (en la página 193)

[Aplicación de reglas de resumen o supresión](#) (en la página 543)

Consideraciones del servicio del incidente

Es posible controlar la forma en la que el servicio del incidente almacena eventos y crea incidentes para un servidor de CA Enterprise Log Manager seleccionado. Puede configurar los siguientes valores:

Hora de caducidad

Especifica la cantidad de tiempo en días que el servicio conserva incidentes en la base de datos de incidentes. Si el valor es 0, los eventos nunca se suprimen. Los incidentes caducados no se muestran.

Valores del límite de generación de incidentes

Especifica la frecuencia con la que una sola regla de correlación puede crear incidentes; lo que le permite reducir varios incidentes no deseados. A efectos de los límites de generación de incidentes, las diferentes versiones de una regla se consideran reglas separadas. De esta forma, si ha aplicado varias versiones de una regla en su entorno, estas se limitan por separado. Los valores de límite incluyen:

Activado

Indica si se aplican los límites de generación de incidentes.

Recuento

Establece un umbral para el número de incidentes generados por una sola regla. Este valor funciona con el valor Hora, si ese valor está por encima de 0. Cuando se alcancen estos números, el servicio del incidente aplica el límite de tiempo bloqueado. De este modo, si establece Recuento como 3, y Hora como 10, el límite se aplica cuando una sola regla genera más de 3 incidentes en 10 segundos.

Hora

Establece un umbral, en segundos, para el número de incidentes generados por una sola regla. Este valor funciona con el valor Recuento, si ese valor está por encima de 0. Cuando se alcancen estos números, el servicio del incidente aplica el límite de tiempo bloqueado. De este modo, si establece Recuento como 3, y Hora como 10, el límite se aplica cuando una sola regla genera más de 3 incidentes en 10 segundos.

Tiempo bloqueado:

Especifica un intervalo en segundos, en los que se bloquea una regla para que no cree más incidentes. Cuando este límite se alcanza, la regla no crea ningún incidente hasta que finalice el tiempo.

Consideraciones sobre el servidor ODBC

El usuario puede instalar un cliente de ODBC o de JDBC para acceder al almacén de registro de eventos de CA Enterprise Log Manager desde una aplicación externa, como Crystal Reports de SAP BusinessObjects.

En la zona de configuración, se pueden llevar a cabo las tareas siguientes:

- Activar o desactivar el acceso de ODBC y JDBC al almacén de registro de eventos.
- Establecer el puerto utilizado para comunicaciones entre el cliente de ODBC o JDBC y el servidor de CA Enterprise Log Manager.
- Especificar si las comunicaciones entre el cliente de ODBC o JDBC y el servidor de CA Enterprise Log Manager estarán cifrados.

Las descripciones de los campos son las siguientes:

Activar servicio

Indica si los clientes de ODBC y JDBC pueden acceder a los datos en el almacén de registro de eventos. Seleccione esta casilla de verificación para activar el acceso externo a los eventos. Anule la selección de la casilla de verificación para desactivar el acceso externo.

Actualmente, el servicio de ODBC no es compatible con FIPS. Si pretende ejecutarlo en el modo FIPS, elimine esta casilla de verificación para prevenir el acceso de ODBC y JDBC. Con ello se previene el acceso no compatible con los datos del evento. Si pretende desactivar el servicio de ODBC y JDBC para las operaciones en modo FIPS, asegúrese de que configura este valor para *cada uno* de los servidores en una federación.

Puerto de escucha del servidor

Especifica el número de puerto utilizado por los servicios de ODBC o JDBC. El valor predeterminado es 17002. El servidor de CA Enterprise Log Manager rechaza los intentos de conexión cuando se especifica un valor diferente en el origen de datos de Windows o en la cadena de la dirección URL de JDBC.

Cifrado (Capa de sockets seguros)

Indica si se debe utilizar cifrado para las comunicaciones entre el cliente de ODBC y el servidor de CA Enterprise Log Manager. El servidor de CA Enterprise Log Manager rechaza los intentos de conexión cuando el valor correspondiente del origen de datos de Windows o la dirección URL de JDBC no coincide con este valor.

Tiempo de espera de sesión (minutos)

Especifica el número de minutos que se mantiene abierta una sesión inactiva antes de que se cierre automáticamente.

Nivel de registro

Define el tipo y el nivel de detalle incluidos en el archivo de registro. La lista desplegable se ordena según el detalle, donde la primera opción ofrece la información menos detallada.

Aplicar a todos los registradores

Controla si la configuración del nivel de registro anula todos los ajustes de registro del archivo de propiedades de registro. Este ajuste sólo se aplica cuando la configuración del nivel de registro es inferior (muestra más detalles) a la configuración predeterminada.

Consideraciones del servidor de informes

El servidor de informes controla la administración de informes enviados de manera automática y su visualización en formato PDF, así como las alertas de acción y la retención de informes. En la zona de configuración del servidor de informes, puede llevar a cabo las tareas siguientes:

- Control del nombre y logotipo de la compañía, contenido y color del encabezado y del pie de página, tipos de letra y otros valores de configuración de los informes en formato PDF desde el área Configuraciones del informe.
- Establecer las alertas de acciones totales retenidas, así como el número de días que se mantendrán en el área de retención de alertas:

Número máximo de alertas de acción

Define el número máximo de alertas de acción que retiene el servidor de informes para su revisión.

Mínimo: 50

Máximo: 1.000

Retención de alertas de acción

Define el número de días durante los que se retienen las alertas de acción, hasta la cantidad máxima indicada.

Mínimo: 1

Máximo: 30

- Establecer la política de retención de cada tipo de repetición de informe programado en el área de retención de informes.
- Establecer la frecuencia con que la utilidad de retención busca informes para eliminarlos de forma automática en función de dichas políticas. Por ejemplo, si la utilidad de retención de informes se ejecuta diariamente, suprimirá los informes diarios con una antigüedad superior a la máxima especificada.

Consideraciones acerca del servicio de prueba de reglas

El servicio de prueba de reglas controla la manera en que CA Enterprise Log Manager comprueba las reglas de correlación. Se pueden establecer los siguientes valores de prueba de reglas.

Límite del evento

Define la cantidad de eventos que se retendrán por incidente cuando se permita la acumulación. El límite de eventos ayuda a evitar el tráfico indebido causado por la correlación en períodos de elevada actividad. Cuando se alcanza este límite, los eventos adicionales se pierden. Por ejemplo, si se establece un límite de 100, cada regla puede acumular hasta 100 eventos registrados, entre los cuales se incluyen los eventos, o evento, iniciales que cumplen los requisitos. La acumulación continúa hasta que se alcanza el límite de eventos o, lo que es más habitual: hasta que los valores de intervalo o límite restablecen la regla.

Número máximo de pruebas de regla simultáneas

Define el número de pruebas de regla que se pueden ejecutar de forma simultánea en un único servidor de CA Enterprise Log Manager.

Consideraciones de la suscripción

Un sistema de servidor proxy/cliente ofrece las actualizaciones de suscripción. El primer servidor instalado se establece como el servidor proxy de suscripción predeterminado, y es el que contacta periódicamente con el servidor de suscripciones de CA para comprobar si hay actualizaciones. Las instalaciones posteriores se configurarán como clientes de dicho servidor proxy y se pondrán en contacto con él de forma periódica para obtener actualizaciones. Si no consiguen ponerse en contacto, se registrará un evento autocontrolado.

El sistema predeterminado reduce el tráfico de red al eliminar la necesidad de que cada servidor se ponga en contacto directo con el servidor de suscripciones de CA y se puede configurar por completo. Puede agregar tantos servidores proxy como necesite.

También puede reducir aún más el tráfico de Internet mediante la creación de servidores proxy sin conexión, que almacenan la información sobre las actualizaciones de forma local y la ofrecen a los clientes cuando se ponen en contacto. Para ofrecer soporte a los servidores proxy sin conexión, copie de forma manual todo el contenido de la ruta de descarga del proxy en línea en la ruta de descarga del proxy sin conexión. Los proxys sin conexión se deben configurar en entornos en los que haya servidores de CA Enterprise Log Manager que no pueden acceder a Internet o a un servidor conectado a Internet.

Al configurar el servicio de suscripción, tenga en cuenta la información siguiente sobre determinados ajustes y sus interacciones:

Proxy de suscripción predeterminado

Define el servidor proxy predeterminado para el servicio de suscripción. El proxy de suscripción predeterminado debe tener acceso a Internet. Si no se define ningún otro proxy de suscripción, este servidor obtiene las actualizaciones de suscripción del servidor de suscripción de CA, descarga las actualizaciones binarias para todos los clientes y distribuye las actualizaciones de contenido entre el almacén de usuarios de CA Enterprise Log Manager. Si se definen otros servidores proxy, los clientes se pondrán en contacto con este servidor para obtener actualizaciones cuando no se haya configurado una lista de servidores proxy de suscripciones o cuando la lista configurada se haya agotado. El valor predeterminado es el primer servidor instalado en el entorno. Este valor sólo está disponible como configuración global.

Clave pública

Define la clave empleada para comprobar y verificar la firma empleada para firmar las actualizaciones. Cuando se actualiza una clave pública-privada, el proxy descarga la actualización al valor de clave pública y actualiza la clave pública. Este valor sólo está disponible como configuración global.

Importante: No actualice este valor manualmente nunca.

¿Proxy de suscripción?

Controla si el servidor local es un proxy de suscripción. Si la casilla de verificación ¿Proxy de suscripción? está sin seleccionar, el servidor es un cliente de suscripción.

Actualizar ahora

Inicia un ciclo de actualización a petición de forma inmediata para el servidor seleccionado. Únicamente puede realizar una actualización a petición para un solo servidor a la vez; esta opción no está disponible globalmente. Actualice un servidor proxy de suscripción antes de actualizar su cliente de suscripción.

Proxy de suscripción en línea

Controla si el servidor local es un proxy de suscripción en línea. Los servidores proxy de suscripción en línea utilizan el acceso a Internet para obtener actualizaciones de suscripción del servidor de suscripción de CA y distribuir las al entorno de CA Enterprise Log Manager. Para designar un servidor como proxy de suscripción en línea, se debe seleccionar tanto la casilla de verificación ¿Proxy de suscripción? como la opción Proxy de suscripción en línea. Este valor sólo está disponible como configuración local.

Proxy de suscripción sin conexión

Controla si el servidor local es un proxy de suscripción sin conexión. Un proxy de suscripción sin conexión es un servidor que obtiene actualizaciones de suscripción a través de una copia de directorios manual (mediante scp) de un proxy de suscripción en línea. Los proxys de suscripción sin conexión no necesitan acceso a Internet. Para designar un servidor como proxy de suscripción sin conexión, se debe seleccionar tanto la casilla de verificación ¿Proxy de suscripción sin conexión? como la opción Proxy de suscripción sin conexión. Este valor sólo está disponible como configuración local.

Nota: Si desea acceder a más información importante sobre la configuración de suscripciones sin conexión, puede consultar la *Guía de administración de CA Enterprise Log Manager*.

URL de fuente RSS

Define la URL del servidor de suscripciones de CA. Los servidores proxy de suscripciones en línea emplean esta URL para acceder al servidor de suscripciones de CA y descargar las actualizaciones de suscripción.

Módulos disponibles para descargar

Le permite seleccionar los módulos que se aplican a su entorno de CA Enterprise Log Manager de entre los módulos disponibles para descargar. Haga clic en Examinar para mostrar este cuadro de diálogo; los módulos que seleccione aparecerán en la lista Módulos.

Los módulos seleccionados se descargan del servidor de suscripción de CA durante actualizaciones de suscripción. Los módulos para descargar se pueden seleccionar a nivel global; otros proxys de suscripción configurados descargan estos módulos de forma predeterminada durante la actualización. Los módulos para descargar también se pueden seleccionar a nivel local para servidores proxy y cliente individuales. Si se realiza esto, se anula la configuración global, de forma que sólo los módulos seleccionados descarguen en el servidor determinado. Los módulos seleccionados para clientes se emplean para actualizar los módulos correspondientes instalados en el cliente. Puede seleccionar un módulo para descargarlo en un cliente aunque no se haya seleccionado como su servidor proxy. El proxy lo recuperará para el cliente, pero no lo instalará en dicho proxy.

Nota: Si el campo está vacío, defina una URL de fuente RSS. Esta configuración permite que el sistema lea la fuente RSS y, en el siguiente intervalo de actualización, muestre la lista de módulos que se pueden descargar.

Módulos seleccionados para la descarga

Muestra los módulos seleccionados en el cuadro de diálogo Explorador de fuentes RSS. El proxy de suscripción predeterminado y el resto de servidores proxy en línea descargan estos módulos del servidor de suscripción de CA durante el proceso de actualización. Los módulos enumerados pueden ser módulos elegidos para descargar a nivel global, o pueden reflejar módulos seleccionados para un servidor determinado a nivel local.

Servidor proxy HTTP

Controla si este servidor se pone en contacto con el servidor de suscripciones de CA a través de un proxy HTTP para obtener las actualizaciones, en lugar de hacerlo directamente.

Dirección proxy que se va a utilizar

Especifica la dirección IP completa del proxy HTTP.

Puerto

Especifica el número de puerto empleado para ponerse en contacto con el proxy HTTP.

Id de usuario del proxy HTTP

Especifica el ID de usuario empleado para ponerse en contacto con el proxy HTTP.

Contraseña de proxy HTTP

Especifica la contraseña empleada para ponerse en contacto con el proxy HTTP.

Programar

Especifica la hora de inicio y frecuencia para que los servidores de CA Enterprise Log Manager soliciten actualizaciones de suscripción. Los servidores proxy de suscripción en línea (incluido el servidor proxy predeterminado) se ponen en contacto con el servidor de suscripción de CA, y los clientes de proxy se ponen en contacto con sus servidores proxy, según esta programación. La programación se puede establecer de forma global para todos los servidores de CA Enterprise Log Manager; también se puede anular de forma local para un servidor determinado.

Proxys de suscripción para las actualizaciones del cliente

Le permite definir los proxys a los que se conectarán todos los clientes o un cliente seleccionado, en una operación por turnos, para obtener actualizaciones del sistema operativo y de los productos. Puede emplear las teclas de flecha hacia arriba/abajo para controlar el orden en el que el cliente se pone en contacto con los servidores proxy de suscripciones. El cliente descarga actualizaciones del primer servidor proxy con el que se conecta de forma correcta. Si ninguno de los servidores proxy configurados está disponible, el cliente se pone en contacto con el proxy de suscripción predeterminado.

Proxys de suscripción para las actualizaciones de contenido

Le permite seleccionar qué servidores proxy se emplean para distribuir actualizaciones de contenido en el almacén de usuarios. Puede seleccionar los servidores proxy sin conexión y en línea. Este valor sólo está disponible como configuración global.

Nota: Por cuestiones de redundancia, baraje la posibilidad de seleccionar más de un servidor que actúe como proxy de suscripción para actualizaciones del contenido.

Más información:

[Espacio libre en disco para actualizaciones](#) (en la página 249)

[Acerca de las claves públicas de suscripción](#) (en la página 250)

Servicio Estado del sistema

El servicio Estado del sistema se puede utilizar para recopilar información acerca de un servidor de CA Enterprise Log Manager, así como para controlarlo. Sólo se puede mostrar el estado del sistema de los servidores de CA Enterprise Log Manager individuales. Toda la configuración y las opciones se aplican en el nivel local.

El servicio Estado del sistema ofrece las fichas siguientes:

- **Administración:** controla los servicios y los servidores de host y crea un archivo de diagnóstico para soporte.
- **Estado:** revisa el estado y la versión de los servicios y los procesos del sistema.
- **Eventos autocontrolados:** revisa los eventos relacionados con el estado del sistema y los componentes.

Más información

[Tareas de estado del sistema](#) (en la página 189)

[Creación de un archivo de diagnóstico para soporte](#) (en la página 190)

[Reinicio de un servidor host](#) (en la página 191)

[Reinicio de los servicios de CA ELM](#) (en la página 191)

[Revisión del estado y la versión del servicio](#) (en la página 192)

[Revisión de los eventos autocontrolados de estado del sistema](#) (en la página 192)

Tareas de configuración de adaptadores de CA

Las escuchas locales reciben y recopilan eventos nativos de determinados tipos de recursos que emplean varios tipos de adaptadores de CA.

Puede ver y editar dos tipos de configuraciones de adaptadores individuales.

- La configuración global se aplica a todas las instancias de un adaptador del entorno, como todas las instancias del recopilador SAPI.
- La configuración local sólo se aplica a un host del adaptador seleccionado, como un recopilador SAPI.

También puede ver eventos de autocontrol de todos los hosts del adaptador o servicios del adaptador desde las áreas de configuración global o local del adaptador en cuestión.

Más información

[Edición de configuraciones de adaptadores globales](#) (en la página 183)

[Edición de configuraciones de adaptadores locales](#) (en la página 184)

[Visualización de eventos autocontrolados del adaptador](#) (en la página 185)

[Visualización del estado del adaptador](#) (en la página 186)

[Consideraciones del servicio de SAPI](#) (en la página 187)

[Consideraciones de iTechnology Event Service](#) (en la página 189)

Edición de configuraciones de adaptadores globales

Puede editar configuraciones de adaptadores globales, que son ajustes que se aplican a todas las instancias de un determinado adaptador de CA en su entorno. Por ejemplo, puede realizar cambios de configuración que se apliquen a todos los recopiladores SAPI ejecutados en el entorno. Las configuraciones de los adaptadores globales *no* anulan las configuraciones del adaptador local que no coincidan con la configuración global.

Para editar configuraciones de adaptadores globales

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la lista de la carpeta Recopilación de registros.
2. Haga clic en la carpeta Adaptadores de CA.
La carpeta se expande y muestra las subcarpetas de cada adaptador.
3. Seleccione la carpeta del adaptador cuya configuración desee editar.
Se abre la pantalla Configuración del servicio global en el panel de detalles.
4. Introduzca los cambios de configuración que desee.

Nota: Al hacer clic en Restablecer, los valores de la configuración se restauran al estado que se guardó más recientemente. Puede restablecer un único cambio o varios cambios hasta el momento en que haga clic en Guardar. Una vez que haya guardado los cambios, deberá restablecerlos de forma individual.

5. Cuando haya terminado de introducir cambios, haga clic en Guardar.
Los cambios de configuración se aplicarán a todos los hosts del adaptador seleccionado, a no ser que tengan configuraciones locales diferentes.

Edición de configuraciones de adaptadores locales

Puede ver o editar las configuraciones de los adaptadores locales. Las configuraciones de adaptadores locales permiten controlar los ajustes que podrían no ser aplicables o necesarios para todo el entorno. Sólo anulan la configuración global de determinados hosts del adaptador. Por ejemplo, puede que quiera que un determinado host del adaptador SAPI escuche un puerto determinado. Puede establecer este comportamiento mediante una configuración local.

Para editar configuraciones de adaptadores globales

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la lista de la carpeta Recopilación de registros.
2. Haga clic en la carpeta Adaptadores de CA.
La carpeta se expande y muestra las subcarpetas de cada adaptador.
3. Seleccione la carpeta del adaptador cuya configuración desee editar.
La pantalla del servicio se amplía y muestra los hosts del adaptador.
4. Haga clic en el host del adaptador que desea.
Se abre la configuración de host seleccionada en el panel de detalles.
5. Introduzca los cambios de configuración que desee. Todos los campos de entrada de valores, menús o controles de la configuración local cuentan con un botón de configuración local/global que se puede establecer en uno de los dos estados.

Configuración global: 

Configuración local: 

Un clic en el botón modifica la configuración de global a local y hace que el campo de entrada asociado esté disponible para su uso. El campo de entrada debe permanecer establecido en la configuración local para que el ajuste tenga efecto: si se establece en la configuración global, se aplicará la configuración global de ese adaptador.

Nota: Al hacer clic en Restablecer, se muestran los valores de configuración almacenados más recientemente para las configuraciones disponibles. Puede restablecer un único cambio o varios cambios hasta el momento en que haga clic en Guardar. Una vez que haya guardado los cambios, deberá restablecerlos de forma individual.

6. Cuando haya terminado de introducir cambios, haga clic en Guardar.

Los cambios que realice sólo se aplicarán al host de adaptador seleccionado.

Visualización de eventos autocontrolados del adaptador

Puede controlar la actividad de los servicios del adaptador y resolver problemas a través de la visualización de los eventos autocontrolados de cada host de servicio del adaptador. Puede ver eventos revisados previamente de las áreas de configuración global o local del adaptador individual.

Para ver eventos autocontrolados del adaptador

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la carpeta Adaptadores de CA.

La carpeta se expande y muestra las subcarpetas de cada servicio del adaptador.

3. Seleccione la carpeta de un servicio del adaptador para visualizar los eventos autocontrolados de dicho servicio o expanda las carpetas y seleccione un host del adaptador para visualizar sólo los eventos autocontrolados de dicho host del adaptador.

La configuración del adaptador aparece en el panel de detalles.

4. Haga clic en la pestaña Eventos autocontrolados.

Aparece una ventana del visor de eventos que muestra los eventos filtrados correctamente. Por ejemplo, si selecciona la carpeta de conexión de eventos de iTechnology en el paso 3, puede ver los eventos autocontrolados de todas las instancias de la conexión de eventos de iTechnology. Si selecciona un host específico en la carpeta de conexión de eventos de iTechnology, sólo puede ver eventos relacionados con dicho host de iTechnology.

Nota: La estructura de su federación controla qué eventos son visibles. Si no se establece ninguna federación, sólo verá eventos locales, independientemente del host seleccionado.

Más información

[Visualización del estado del adaptador](#) (en la página 186)

[Edición de configuraciones de adaptadores globales](#) (en la página 183)

[Edición de configuraciones de adaptadores locales](#) (en la página 184)

Visualización del estado del adaptador

Puede visualizar el estado actual de algunos servicios del adaptador de CA, incluida la hora de inicio, el estado de ejecución, así como las estadísticas y la información de envío de eventos. No puede ver el estado del servicio de conexión de eventos de iTechnology.

Para visualizar el estado del adaptador

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la carpeta Adaptadores de CA.

La carpeta se expande y muestra las subcarpetas de cada servicio del adaptador.

3. Seleccione la carpeta del adaptador cuyo estado desee visualizar.

La pantalla del servicio se amplía y muestra los hosts del adaptador individuales.

4. Haga clic en el host del adaptador que desea.

Se abre la configuración de host seleccionada en el panel de detalles.

5. Haga clic en la ficha Estado.

Aparece la información de estado.

Nota: La información de estado sólo aparece en el panel de configuración local.

Consideraciones del servicio de SAPI

CA Enterprise Log Manager emplea dos instancias del servicio de interfaz de programación de envío de aplicaciones (SAPI) CA Audit, una instalada como recopilador de SAPI y la otra como enrutador de SAPI. Los servicios de SAPI se suelen emplear para recibir eventos de productos integrados y de clientes de CA Audit existentes. Puede configurar los adaptadores de SAPI mediante los ajustes siguientes:

Activar escucha

Activa el servicio seleccionado. Este ajuste está activado de forma predeterminada.

Puerto SAPI

Define un número de puerto determinado para el servicio seleccionado si no está registrado mediante el asignador de puertos. El valor predeterminado, 0, permite que el servicio utilice un puerto determinado de forma aleatoria si se selecciona la casilla de verificación Registrar.

Nota: El número de puerto debe ser diferente para el recopilador y el enrutador SAPI. Si se establece el mismo puerto para ambos servicios, el que se haya definido en segundo lugar no funcionará.

Registrar

Controla si el servicio se registra con el asignador de puertos del sistema. Si selecciona Registrar e introduce 0 en el campo Puerto SAPI, se selecciona un puerto cualquiera cada vez que se inicia el servicio. Ésta es la configuración predeterminada para ambos campos. Si no selecciona Registrar, debe especificar un puerto SAPI.

Clave de cifrado

Define la clave de cifrado, si utiliza una clave de cifrado no estándar en el entorno de CA Audit, que emplea el adaptador SAPI para leer eventos SAPI entrantes.

Orden de eventos

Garantiza que los eventos se envían al sistema de almacenamiento de registro de eventos en el mismo orden en el que se reciben. Si se desactiva el orden de eventos, el orden podrá modificarse si unos eventos se analizan y se envían más rápido que otros. La activación del orden de eventos puede afectar al rendimiento aumentando el tamaño de la cola de eventos.

Límite de eventos

Define el número máximo de eventos en la cola de procesamiento de eventos y permite el control de los recursos de procesamiento. Si se introduce el valor 0 en este campo, no se aplica ningún límite. Los eventos que superen el límite, se retrasarán en el origen.

Recuento de subprocesos por cola

Define el número de subprocesos en procesamiento de cada protocolo. El empleo de varios subprocesos en procesamiento agilizará el procesamiento si se desactiva el orden de eventos. Si el orden de eventos está activado, el recuento de subprocesos no tendrá ningún efecto. El empleo de muchos subprocesos puede tener implicaciones en el rendimiento.

Asignación de datos y cifrados

- El control de cambio de cifrados determina cuál de los cifrados disponibles empleará el servicio para descifrar los mensajes entrantes.
- El control de cambio de archivos de asignación de datos determina cuál de los archivos de asignación de datos disponibles empleará el servicio para asignar los eventos.

La configuración de registro controla el modo en que los módulos de CA Enterprise Log Manager individuales registran los mensajes internos. Sólo está disponible como configuración local. La configuración de registro se suele emplear para solucionar problemas. Normalmente, no hay que modificar esta configuración y sólo tendrá que conocer bien el registro y los archivos de registro antes de realizar modificaciones.

Nivel de registro

Define el tipo y el nivel de detalle incluidos en el archivo de registro. La lista desplegable se ordena según el detalle, donde la primera opción ofrece la información menos detallada y la última ofrece la más detallada.

Aplicar a todos los registradores

Controla si la configuración del nivel de registro anula todos los ajustes de registro del archivo de propiedades de registro. Este ajuste sólo se aplica cuando la configuración del nivel de registro es inferior (muestra más detalles) a la configuración predeterminada.

Consideraciones de iTechnology Event Service

El servicio de iTechnology controla los eventos enviados a través del daemon de iGateway. Puede configurar el servicio estableciendo cuál de los archivos de asignación de datos (DM) disponibles será el que empleará el servicio para la asignación de eventos mediante el control de cambio de archivos de DM.

El servicio de conexión de eventos está preconfigurado para incluir la mayor parte de los archivos de asignación de datos más grandes.

La configuración de registro controla el modo en que los módulos de CA Enterprise Log Manager individuales registran los mensajes internos. Sólo está disponible como configuración local. La configuración de registro se suele emplear para solucionar problemas. Normalmente, no hay que modificar esta configuración y sólo tendrá que conocer bien el registro y los archivos de registro antes de realizar modificaciones.

Nivel de registro

Define el tipo y el nivel de detalle incluidos en el archivo de registro. La lista desplegable se ordena según el detalle, donde la primera opción ofrece la información menos detallada, y la última ofrece la más detallada.

Aplicar a todos los registradores

Controla si la configuración del nivel de registro anula todos los ajustes de registro del archivo de propiedades de registro. Este ajuste sólo se aplica cuando la configuración del nivel de registro es inferior (muestra más detalles) a la configuración predeterminada.

Tareas de estado del sistema

Desde el servicio Estado del sistema puede realizar las siguientes acciones:

- Revisar el estado y la versión de los servicios del sistema.
- Revisar los eventos autocontrolados relacionados con los componentes y el uso del sistema.
- Crear un archivo de diagnóstico para soporte.
- Reiniciar los servicios de CA ELM.
- Reiniciar el servidor host en el que se esté ejecutando un servidor de CA Enterprise Log Manager.
- Activar la operación en modo FIPS o no-FIPS.

Más información:

[Creación de un archivo de diagnóstico para soporte](#) (en la página 190)

[Reinicio de un servidor host](#) (en la página 191)

[Reinicio de los servicios de CA ELM](#) (en la página 191)

[Revisión del estado y la versión del servicio](#) (en la página 192)

[Revisión de los eventos autocontrolados de estado del sistema](#) (en la página 192)

Creación de un archivo de diagnóstico para soporte

Puede revisar el estado y la versión de los servicios que se ejecutan en un servidor de CA Enterprise Log Manager seleccionado. Al hacer clic en Diagnóstico para soporte se ejecutará el script de LmDiag.sh que se proporciona con CA Enterprise Log Manager.

Esta utilidad empaqueta la información del sistema y los archivos de registro en un archivo .tar comprimido para transmitirla al personal de Soporte de CA. Para transferir este archivo puede utilizar FTP o cualquier otro método de transferencia de archivos.

Nota: Una parte de la información del archivo resultante puede ser confidencial como, por ejemplo, las direcciones IP, las configuraciones del sistema, los registros del hardware y los registros de procesos. Utilice un método seguro para almacenar y transportar este archivo.

Para crear un archivo de diagnóstico

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la entrada Estado del sistema.
3. Seleccione un servidor específico de CA Enterprise Log Manager.
La configuración del servicio de estado del sistema mostrará la ficha Administración.
4. Haga clic en Diagnóstico para soporte.
5. Seleccione una ubicación de archivo para la descarga del archivo de diagnóstico generado.

La utilidad crea el archivo y lo descarga en la ubicación especificada y se cierra automáticamente una vez que se ha copiado el archivo.

Reinicio de un servidor host

Puede revisar el estado y la versión de los servicios que se ejecutan en un servidor de CA Enterprise Log Manager seleccionado.

Importante: Esta función sólo se debe utilizar cuando sea necesario o cuando se lo indique el Soporte de CA. Como resultado del reinicio del servidor de CA Enterprise Log Manager, éste deja de recibir, analizar y almacenar registros de eventos hasta que finaliza el reinicio. Si reinicia el servidor de gestión, las sesiones gestionadas de CA Enterprise Log Manager de otros servidores asociados deberán cerrar sesión e iniciarla de nuevo.

Para reiniciar un servidor host

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la entrada Estado del sistema.
3. Seleccione un servidor específico de CA Enterprise Log Manager.
La configuración del servicio de estado del sistema mostrará la ficha Administración.
4. Haga clic en Reiniciar Host.

Reinicio de los servicios de CA ELM

Puede reiniciar los servicios de CA ELM que se ejecutan en un servidor de CA Enterprise Log Manager seleccionado.

Importante: Esta función sólo se debe utilizar cuando sea necesario o cuando se lo indique Soporte de CA. Como resultado del reinicio de los servicios de CA ELM, el servidor de CA Enterprise Log Manager afectado deja de recibir, analizar y almacenar registros de eventos hasta que finaliza el reinicio. Si reinicia el servidor de gestión, la sesión actual y todas las demás sesiones de CA Enterprise Log Manager de otros servidores deberán cerrar sesión e iniciarla de nuevo.

Para reiniciar los servicios de CA ELM.

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la entrada Estado del sistema.
3. Seleccione un servidor específico de CA Enterprise Log Manager.
La configuración del servicio de estado del sistema mostrará la ficha Administración.
4. Haga clic en Volver a iniciar servicios de CA ELM.

Revisión del estado y la versión del servicio

Puede revisar el estado y la versión de los servicios que se ejecutan en un servidor de CA Enterprise Log Manager seleccionado.

Para revisar el estado

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la entrada Estado del sistema.
3. Seleccione un servidor específico de CA Enterprise Log Manager.
4. Haga clic en la ficha Estado.

Revisión de los eventos autocontrolados de estado del sistema

Puede revisar el estado y la versión de los servicios que se ejecutan en un servidor de CA Enterprise Log Manager seleccionado. Los mensajes de estado incluyen eventos relacionados con el uso del procesador y del espacio en disco, los promedios de carga de la CPU, el uso de la memoria, el acceso y el uso del hardware y otros eventos.

Para revisar los eventos autocontrolados

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la entrada Estado del sistema.
3. Seleccione un servidor específico de CA Enterprise Log Manager.
4. Haga clic en la ficha Eventos autocontrolados.

Capítulo 6: Almacenamiento de registros

Esta sección contiene los siguientes temas:

[Acerca del almacenamiento de registros](#) (en la página 194)

[Estados de la base de datos de registro de eventos](#) (en la página 196)

[Copia de seguridad y restauración de ACS](#) (en la página 199)

[Comprobaciones de la integridad de datos](#) (en la página 200)

[Configuración de autenticaciones no interactivas para su restauración](#) (en la página 204)

[Consulta del catálogo de archivado](#) (en la página 211)

[Restauración de archivos almacenados de forma automática](#) (en la página 213)

[Script de restauración para restaurar bases de datos almacenadas](#) (en la página 214)

[Copia de seguridad manual de bases de datos archivadas](#) (en la página 217)

[Restauración manual de archivos en el sistema de almacenamiento de registro de eventos original](#) (en la página 221)

[Restauración manual de archivos en sistemas de almacenamiento de registro de eventos nuevos](#) (en la página 228)

[Seguimiento de copia de seguridad/restauración de LMArchive](#) (en la página 232)

Acerca del almacenamiento de registros

Puede gestionar dos aspectos del almacenamiento de eventos a través de CA Enterprise Log Manager:

- Copia de seguridad de las bases de datos de archivos de registro situadas en el directorio de archivo de cada servidor de informes en un directorio de archivo creado en un servidor de almacenamiento remoto. El servidor de almacenamiento remoto es una ubicación interna para guardar las bases de datos almacenadas hasta que se puedan trasladar a un emplazamiento externo.
- Restauración de las bases de datos de archivos de registro desde el directorio de archivo de un servidor de almacenamiento remoto hasta el servidor de informes original o un servidor de CA Enterprise Log Manager designado como servidor de punto de restauración. Una vez restauradas, puede examinar el contenido mediante consultas e informes.

Puede gestionar las copias de seguridad de las bases de datos de registro de eventos de dos maneras:

- (Preferido) Configure el servidor de CA Enterprise Log Manager para utilizar el almacenamiento automático para desplazar bases de datos tibias de un servidor de informes de CA Enterprise Log Manager a un servidor de almacenamiento remoto de forma programada. El proceso de almacenamiento automático informa al servidor de informes de que se han realizado las copias de seguridad de las bases de datos.

Nota: Consulte "Acerca del almacenamiento automático" en la *Guía de implementación de CA Enterprise Log Manager*.

- Realice copia de seguridad de las bases de datos del servidor de CA Enterprise Log Manager manualmente y cópielas a una ubicación de almacenamiento interno. Utilice la utilidad LMArchive para notificar al servidor de CA Enterprise Log Manager para que introduzca una marca que permite identificar que se ha realizado una copia de seguridad de estas bases de datos.

El traslado de los archivos con copia de seguridad a una ubicación externa es una tarea que se lleva a cabo fuera del servidor de CA Enterprise Log Manager, al igual que la tarea de retorno a la red cuando es necesario para realizar la restauración.

Puede realizar consultas en el catálogo de archivo para identificar los archivos de bases de datos que desea restaurar. Puede restaurar las bases de datos según lo necesite de dos maneras:

- Puede restaurarlas en el servidor de informes original a través de uno de los métodos siguientes:

- Si configura la autenticación no interactiva entre el servidor de almacenamiento remoto y el servidor de informes original, ejecute el script de `restore-ca-elm.sh` para restaurar las bases de datos archivadas al servidor de informes original.

Una vez que se hayan restaurado los archivos, realice consultas e informes durante los días configurados para la duración de los archivos tibios.

- Si ha realizado las copias de seguridad de las bases de datos de archivo de forma manual, copie los archivos de nuevo en el mismo directorio de archivo y, a continuación, informe de la restauración al servidor de CA Enterprise Log Manager. Puede utilizar una opción de la utilidad de línea de comandos `LMArchive` para informar al servidor de CA Enterprise Log Manager que las bases de datos están restauradas.

Una vez que se hayan restaurado los archivos, realice consultas e informes durante el tiempo en horas configurado para la duración de los archivos descongelados.

- Se pueden restaurar bases de datos archivadas a un servidor de punto de restauración dedicado a examinar registros de eventos restaurados, con cualquiera de los métodos siguientes.
 - Si se configura la autenticación no interactiva desde el servidor de almacenamiento remoto al punto de restauración de CA Enterprise Log Manager, se puede ejecutar el script `restore-ca-elm.sh` para restaurar bases de datos archivadas hasta el punto de restauración.
 - Si no se ha configurado la autenticación no interactiva, se deberán copiar manualmente las bases de datos de archivo del servidor de almacenamiento remoto al directorio de archivo del servidor de punto de restauración. A continuación, informe al servidor de CA Enterprise Log Manager de la restauración mediante la función `Recatalogar` de la consulta de catálogo de archivos en el explorador de recopilación de registros.

Esta notificación tiene como resultado la reconstrucción del catálogo, que hace que los archivos de la base de datos estén disponibles para realizar consultas e informes. Esta disponibilidad depende de que la antigüedad en días configurada para los archivos tibios antes de su eliminación se haya establecido en un valor que supere la antigüedad de los archivos restaurados. Por lo tanto, es importante que la antigüedad máxima de los archivos tibios se establezca correctamente en cualquier punto de restauración indicado.

Estados de la base de datos de registro de eventos

Cuando configura el archivo automático en tres servidores (recopilación, informe y almacenamiento remoto), todas las bases de datos de registro de eventos atraviesan tres estados: caliente, tibio y frío. Con esta arquitectura, las bases de datos calientes de registros sin comprimir sólo existen en el servidor de recopilación. El servidor de informes guarda las bases de datos tibias; el servidor de almacenamiento remoto sólo guarda las bases de datos frías. Cuando se restaura una base de datos fría mediante script shell de restauración, se restaura en estado caliente. Si se restaura de forma manual mediante la utilidad LMArchive, se restaura en estado descongelado.

Los siguientes cuatro estados de almacenamiento de registro de eventos describen bases de datos descomprimidas, comprimidas, a las que se ha realizado una copia de seguridad y restauradas respectivamente:

Caliente

El *estado caliente de base de datos* es el estado de la única base de datos descomprimida en el sistema de almacenamiento de registro de eventos de un servidor de recopilación en el que se insertan eventos recién procesados. Puede configurar el número máximo de registros nuevos que desea almacenar en una base de datos caliente (Número máximo de filas) antes de comprimirla en forma de base de datos tibia. Puede programar el archivo automático para desplazar cada hora las bases de datos tibias del servidor de recopilación al servidor de informes configurado. (También existe una base de datos en el servidor de informes para insertar eventos autocontrolados.)

Tibio

El *estado tibio de base de datos* es el estado de las bases de datos retenidas en el sistema de almacenamiento de registro de eventos del servidor de informes. Si configura un archivo automático diario entre el servidor de informes y un servidor de almacenamiento remoto, las bases de datos tibias se retienen hasta que se trasladen al servidor de almacenamiento remoto; a continuación, se eliminan de forma automática del servidor de informes. Si no configura un archivo automático entre el servidor de informes y un servidor de almacenamiento remoto, las bases de datos tibias pueden permanecer en el servidor de informes hasta que los días de permanencia alcancen el valor configurado del número máximo de días de archivado o cuando se alcance el umbral configurado de espacio en disco para archivo, lo que suceda en primer lugar. Al alcanzar uno de los umbrales, la base de datos se elimina y su estado pasa a frío. Sin archivo automático, debe realizar una copia de seguridad manual de las bases de datos tibias con una herramienta de otro fabricante antes de que se eliminen y, a continuación, ejecutar la utilidad LMArchive para indicar a CA Enterprise Log Manager los nombres de las bases de datos de las que se han hecho copias de seguridad y que se han trasladado. El estado tibio también se aplica cuando se realiza una recatalogación mediante el script `restore-ca-elm.sh` o el botón Recatalogar tras restaurar una base de datos fría.

Frío

El *estado base de datos fría* se aplica a una base de datos situada en el servidor de almacenamiento remoto. El registro de una base de datos fría se crea en el servidor de informes cuando la base de datos se almacena de forma automática en el servidor de gestión remota y se elimina del servidor de informes. Si se maneja de forma manual, se crea un informe de la base de datos fría al ejecutar la utilidad LMArchive con la opción `-notify arch`. Puede enviar consultas al catálogo de archivos de un servidor de informes para identificar las bases de datos frías que desea restaurar.

Descongelado

El *estado descongelado de base de datos* es el estado aplicado a una base de datos fría física que se ha restaurado en el directorio de archivo después de que el administrador haya ejecutado la utilidad LMArchive con la opción `-notify rest` para notificar a CA Enterprise Log Manager que se ha restaurado. Las bases de datos descongeladas se retienen durante el número de horas configurado en la política de exportación.

Puede realizar consultas en las bases de datos en cualquiera de los estados. Las consultas normales devuelven datos de eventos de las bases de datos calientes y tibias del servidor de informes y de las bases de datos descongeladas si las hay. Las consultas federadas devuelven datos de eventos de todos los servidores de la federación, incluidos los servidores de recopilación federados que contienen bases de datos calientes. Las consultas de archivos devuelven una lista de las bases de datos que ya no figuran en el servidor de informes, es decir, bases de datos en estado frío. Las bases de datos físicas representadas por una consulta de archivos pueden figurar en el servidor de almacenamiento remoto empleado para el almacenamiento interno o externo.

Más información

[Copia de seguridad y restauración de ACS](#) (en la página 199)

[Copia de seguridad manual de bases de datos archivadas](#) (en la página 217)

[Restauración manual de archivos en el sistema de almacenamiento de registro de eventos original](#) (en la página 221)

[Restauración manual de archivos en sistemas de almacenamiento de registro de eventos nuevos](#) (en la página 228)

Copia de seguridad y restauración de ACS

Un proceso de copia de seguridad garantiza que no se pierden datos debido a la supresión de bases de datos antiguas. El método más recomendado para crear copias de seguridad de bases de datos guardadas es emplear el almacenamiento automático. El archivado automático es un traslado programado y automatizado de bases de datos archivadas entre pares de servidores. El archivado automático entre un servidor de origen y un servidor de destino requiere la autenticación no interactiva. La autenticación no interactiva utiliza la autenticación de clave pública RSA sin una frase de contraseña. Se puede configurar la autenticación no interactiva y el archivado automático:

- De cada servidor de recopilación a su servidor de informes.
- De cada servidor de informes a su servidor de almacenamiento remoto.

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

Un proceso de restauración desplaza bases de datos archivadas de un servidor de almacenamiento remoto al servidor de CA Enterprise Log Manager para fines investigativos. El método preferido para restaurar bases de datos archivadas es utilizar el script `restore-ca-elm.sh`. Esta utilidad de restauración automatiza el traslado de bases de datos archivadas. Como en el caso del proceso de archivado automático, el script `restore-ca-elm.sh` utiliza la autenticación no interactiva. Es posible configurar la autenticación no interactiva y ejecutar el script de restauración:

- Del servidor de almacenamiento remoto a cada servidor de informes original.
- Del servidor de almacenamiento remoto a un único servidor de punto de restauración.

El archivado automático se configura de manera que se produzca de forma programada periódicamente. La restauración se invoca según resulte necesaria.

Comprobaciones de la integridad de datos

Es posible comprobar datos archivados o recatalogados para manipularlos si inicia sesión como un usuario con derechos de administrador. Estas comprobaciones le permiten asegurar sus datos archivados, y cumplir con los requisitos legales. CA Enterprise Log Manager utiliza firmas electrónicas para validar las bases de datos. Si se corrompe la base de datos, o si falta o se corrompe la firma, la comprobación de la integridad de datos determina que la base de datos está manipulada.

Puede configurar las comprobaciones de la integridad de datos de las siguientes maneras:

- De forma automática al restaurar y recatalogar datos
- En horas programadas para servidores seleccionados
- A petición cuando lo desee

Se pueden consultar los resultados de cualquiera de estas comprobaciones en la interfaz Integridad de datos. Cualquier base de datos que haya sido manipulada se pone en cuarentena, y aparece en la lista Bases de datos en cuarentena.

Más información:

[Activación de comprobación de la integridad automática](#) (en la página 200)

[Programación de una comprobación de la integridad de datos](#) (en la página 201)

[Comprobación de la integridad de datos a petición](#) (en la página 201)

[Firma de bases de datos en cuarentena](#) (en la página 202)

Activación de comprobación de la integridad automática

Puede establecer una comprobación de la integridad de datos para que se efectúe automáticamente al restaurar o recatalogar datos.

Para activar una comprobación de la integridad de datos automática

1. Haga clic en la ficha Administración y, a continuación, expanda la subficha Servicios.
2. Seleccione el nodo Almacén de registro de eventos para activar las comprobaciones automáticas globales, o expanda el nodo Almacén de registro de eventos y seleccionar un servidor de CA Enterprise Log Manager para activar una comprobación automática local.
3. Seleccione Validar la integridad al recatalogar y restaurar.

Programación de una comprobación de la integridad de datos

Se pueden programar comprobaciones de la integridad de datos diarias para que se efectúe en horas establecidas y en servidores de CA Enterprise Log Manager seleccionados. Toda base de datos manipulada que se detecte durante una comprobación de la integridad programada se pone automáticamente en cuarentena.

Para programar una comprobación de la integridad de datos

1. Haga clic en la ficha Administración y, a continuación, expanda la subficha Servicios.
2. Seleccione el nodo Almacén de registro de eventos para programar una comprobación global, o expanda el nodo Almacén de registro de eventos y seleccione un servidor de CA Enterprise Log Manager para establecer una comprobación local.
3. Seleccione Activado.
4. (Opcional) Seleccione Federado para ejecutar la comprobación programada en cualquier servidor federado visible desde el servidor seleccionado.
5. Establezca la hora de inicio diaria.

Comprobación de la integridad de datos a petición

Es posible ejecutar una comprobación de la integridad de datos en cualquier momento en un servidor de CA Enterprise Log Manager seleccionado.

Para ejecutar una comprobación de la integridad de datos a petición

1. Haga clic en la ficha Administración y en la subficha Gestión de archivos.
2. Expanda la carpeta Integridad de datos, y seleccione el servidor de CA Enterprise Log Manager donde en el que desee realizar una comprobación.
3. Seleccione un intervalo de tiempo para la comprobación.
4. (Opcional) Seleccione Federado para ejecutar la comprobación en cualquier servidor federado visible para el servidor seleccionado.
5. Haga clic en Validar ahora.

Aparecerá una lista de las bases de datos comprobadas. Cualquier base de datos manipulada que se detecte se mostrará con un icono rojo. También aparecerán en la lista Bases de datos en cuarentena.

Firma de bases de datos en cuarentena

Es posible regenerar la firma electrónica en una base de datos en cuarentena, de forma que esté disponible para consultas.

Para regenerar una firma de base de datos en cuarentena

1. Haga clic en la ficha Administración y en la subficha Gestión de archivos.
2. Expanda la carpeta Integridad de datos, y seleccione el servidor de CA Enterprise Log Manager en el que se encuentren las bases de datos en cuarentena.
3. Haga clic en la ficha Bases de datos en cuarentena en el panel derecho.
4. Seleccione la base de datos para la que desee regenerar una firma.
5. Haga clic en Generar firma.

Aparece un mensaje de confirmación.

Alternancia de claves

Puede alternar las claves de registro utilizadas para asegurar bases de datos archivadas para mejorar la seguridad.

Las claves de registro utilizan una combinación de clave de cifrado pública/privada para asegurar los archivos de las bases de datos. Cuando se alternan claves, la clave pública antigua se conserva, para que CA Enterprise Log Manager pueda verificar archivos que utilizaban la clave privada antigua.

Para alternar claves de registro

1. Haga clic en la ficha Administración y, a continuación, expanda la subficha Servicios.
 2. Seleccione la carpeta Integridad de datos, y haga clic en Alternar claves
- Aparecerá un mensaje de confirmación.

Importación de claves

Es posible importar claves de registro públicas utilizadas para asegurar bases de datos archivadas desde un origen externo. Las importaciones le permiten conservar claves utilizadas por otros servidores de CA Enterprise Log Manager más antiguos, o por servidores anteriores. Por ejemplo, si conserva una lista de copia de seguridad de claves públicas, podría realizar una importación para poder verificar firmas de bases de datos antiguas en un servidor de CA Enterprise Log Manager recién creado.

Para importar claves de registro

1. Haga clic en la ficha Administración y, a continuación, expanda la subficha Servicios.
2. Seleccione la carpeta Integridad de datos, y haga clic en Importar claves.
Aparecerá un cuadro de diálogo de importación de archivo.
3. Busque el archivo de clave XML que desee importar y haga clic en Aceptar.
Aparecerá un mensaje de confirmación.

Nota: Únicamente puede importar claves en formato XML.

Exportación de claves

Es posible exportar las claves de registro públicas utilizadas para asegurar bases de datos archivadas. La exportación le permite realizar copias de seguridad de las claves para importarlas posteriormente a otros servidores de CA Enterprise Log Manager.

Para exportar claves de registro

1. Haga clic en la ficha Administración y, a continuación, expanda la subficha Servicios.
2. Seleccione la carpeta Integridad de datos, y haga clic en Exportar claves.
Aparecerá un cuadro de diálogo de exportación.
3. Seleccione la ubicación que desee y haga clic en Guardar.

Configuración de autenticaciones no interactivas para su restauración

Tras configurar la autenticación ssh no interactiva entre el servidor de almacenamiento remoto y el servidor de destino, se puede utilizar el script shell `restore-ca-elm` para restaurar las bases de datos de archivo a petición. Para la restauración, el servidor de almacenamiento remoto es el origen mientras que el servidor de informes de CA Enterprise Log Manager o el servidor de punto de restauración de CA Enterprise Log Manager es el destino.

Los procesos son un poco diferentes, en función de si el destino es un servidor de informes o un servidor de punto de restauración dedicado.

- Si se utiliza un servidor de punto de restauración dedicado, se debe establecer una vez la autenticación no interactiva que se utilizará para cada restauración. El procedimiento configura el directorio `.ssh` en el punto de restauración con la propiedad necesaria y establece los permisos en el archivo de clave.
- Si se restauran bases de datos de archivo desde el servidor de almacenamiento remoto en varios servidores de informes, se establece la autenticación no interactiva entre cada par de servidores. Se crea el par de claves una vez, pero se copia la misma clave pública de este par de claves para cada servidor de informes de destino. Por ejemplo, se puede copiar la clave pública del servidor de almacenamiento remoto en cada servidor de informes con el nombre `authorized_keys_RSS`. En cada servidor de informes, se deberá concatenar el archivo `authorized_keys_RSS` en el archivo `authorized_keys` existente. El archivo existente contiene las claves públicas copiadas de cada servidor de recopilación.

Ambos procesos asumen que previamente se ha preparado el servidor de almacenamiento remoto para que actúe como el servidor de destino para el archivado automático, lo cual requiere la autenticación no interactiva. Si no se ha efectuado esta preparación, consulte el tema *Creación de una estructura de directorios con propiedades en un servidor de almacenamiento remoto*, en la *Guía de implementación* para obtener más detalles.

Ejemplo: configuración de la autenticación desde un servidor de almacenamiento remoto a un servidor de punto de restauración

Si se utiliza un servidor de CA Enterprise Log Manager como servidor de punto de restauración dedicado resulta fácil establecer la autenticación no interactiva. Una vez se ha realizado la configuración entre el servidor de almacenamiento remoto y el punto de restauración, se puede utilizar el script `restore-ca-elm.sh` en cada restauración sin tener que realizar otros pasos para la autenticación.

El proceso de configuración de la autenticación no interactiva desde un servidor de almacenamiento a un punto de restauración de CA Enterprise Log Manager conlleva los siguientes procedimientos.

1. En el servidor de almacenamiento remoto, debe generar el par de claves pública/privada RSA. Copie la clave pública con el nombre `authorized_keys` en el directorio `/tmp` en el punto de restauración.
2. En el punto de restauración, cree el directorio `.ssh` dentro de `/opt/CA/LogManager` y establezca la propiedad para `caelmservice`. Copie `authorized_keys` del directorio `/tmp` en el directorio `.ssh`. Modifique la propiedad y establezca los permisos en `authorized_keys`.
3. Compruebe la autenticación no interactiva entre el servidor de almacenamiento remoto y el punto de restauración.

Generación de claves y copiado de la clave pública en el punto de restauración

Desde el servidor de almacenamiento remoto, se deben generar un par de claves RSA con el usuario caelmservice. A continuación, se debe realizar una copia del archivo de clave pública id_rsa.pub en el directorio /tmp del punto de restauración de CA Enterprise Log Manager y nombrarlo authorized_keys. Un punto de restauración es un servidor dedicado a investigar datos restaurados.

Se asume que la estructura del directorio /opt/CA/LogManager/.ssh también existe en el servidor de almacenamiento y que la propiedad de éste está establecida en el usuario y grupo caelmservice. Contiene el archivo authorized_keys que se ha copiado de los servidores de informes. Cuando se genera un par de claves, se debe guardar el archivo id_rsa.pub en el directorio /opt/CA/LogManager/ssh.

Para generar el par de claves pública/privada RSA para la autenticación desde un servidor de almacenamiento remoto a un servidor de punto de restauración

1. Inicie sesión en el servidor remoto empleado para el almacenamiento a través de ssh como usuario caelmadmin.
2. Cambie los usuarios a la cuenta raíz.

su –
3. Cambie los usuarios a la cuenta de caelmservice.

su – caelmservice
4. Genere un par de claves RSA como usuario caelmservice.

ssh-keygen -t rsa
5. Pulse Intro para aceptar los valores predeterminados cuando aparezcan las siguientes solicitudes:
 - Introduzca el archivo donde se guardará la clave (/opt/CA/LogManager/.ssh/id_rsa):
 - Introduzca la frase de contraseña (queda vacío si no se utiliza frase de contraseña):
 - Introduzca de nuevo la misma frase de contraseña:
6. Cambie los directorios a /opt/CA/LogManager.
7. Cambie los permisos del directorio .ssh utilizando el siguiente comando.

chmod 755 .ssh

8. Vaya a `.ssh`, donde se guardará la clave `id_rsa.pub`.

```
cd .ssh
```

9. Copie la clave pública con el nombre `authorized_keys` en el directorio `/tmp` en el punto de restauración.

```
scp id_rsa.pub caelmadmin@<restore_point>:/tmp/authorized_keys
```

Preparación del archivo de clave pública para su utilización

Se debe crear el directorio `.ssh` en el servidor de punto de recuperación y establecer la propiedad en `caelmservice`. Posteriormente, se debe copiar `authorized_keys` del directorio `/tmp` en el directorio `.ssh`. Por último, se debe establecer la propiedad y los permisos en el archivo de clave pública.

Para preparar la clave pública en el servidor de punto de restauración para la autenticación no interactiva

1. Inicie sesión en el servidor de punto de restauración de CA Enterprise Log Manager a través de `ssh` como usuario `caelmadmin`.
2. Cambie los usuarios a `root`.
3. Modifique los directorios por el directorio de CA Enterprise Log Manager.

```
cd /opt/CA/LogManager
```

4. Cree el directorio `.ssh`:

```
mkdir .ssh
```

5. Modifique la propiedad de `.ssh` y establézcala para el usuario y grupo `caelmservice`:

```
chown caelmservice:caelmservice .ssh
```

6. Modifique los directorios a `/opt/CA/LogManager/.ssh`.

7. Copie el archivo `authorized_keys` de `/tmp` a `.ssh`:

```
cp /tmp/authorized_keys .
```

8. Modifique la propiedad del archivo `authorized_keys` y establézcala para `caelmservice`:

```
chown caelmservice:caelmservice authorized_keys
```

9. Modifique los permisos en el archivo `authorized_keys`:

```
chmod 755 authorized_keys
```

Ejemplo: configuración de la autenticación de un servidor de almacenamiento a un servidor de informes

Se pueden restaurar bases de datos archivadas desde un servidor de almacenamiento remoto de vuelta a su servidor de informes original, es decir, al servidor desde dónde fueron archivadas automáticamente. La ventaja de este método es que no es necesario recatalogar la base de datos de archivo de CA Enterprise Log Manager. El servidor de informes ya sabe cuáles son las bases de datos de archivos de registro que se están restaurando. Si dispone de varios servidores de informes, configure la autenticación no interactiva entre el servidor de almacenamiento remoto y cada servidor de informes. El archivo `authorized_keys` se encuentra en el directorio `.ssh` del servidor de informes. Este archivo `authorized_keys` tiene las claves públicas de todos los pares claves generados por un servidor de recopilación que archive automáticamente a este servidor de informes. Por lo tanto, se crea un archivo de claves autorizadas con un sufijo y a continuación se concatena ese archivo al archivo `authorized_keys` original.

El proceso de configuración de la autenticación no interactiva desde un servidor de almacenamiento remoto a un servidor de informes de CA Enterprise Log Manager conlleva los siguientes procedimientos.

1. En el servidor de almacenamiento remoto:
 - a. Configure el par de claves pública/privada RSA para la autenticación de almacenamiento remoto a servidor de informes.
 - b. Copie la clave pública del servidor de almacenamiento al directorio `/tmp` del servidor de informes con el nombre `authorized_keys_RSS`.
2. En el servidor de informes:
 - a. Copie el archivo `authorized_keys` actual de `.ssh` a `/tmp`.
 - b. Concatene `authorized_keys_RSS` del directorio `/tmp` con el archivo `authorized_keys`.
 - c. Vuelva a copiar el archivo `authorized_keys` al que se han anexado datos en el directorio `.ssh`.
3. En el servidor de almacenamiento remoto, compruebe que la autenticación no interactiva se realiza correctamente entre servidores.
4. Repita estos pasos para cada combinación de servidor de almacenamiento remoto a servidor de informes.

Generación de claves y copiado de claves públicas en los servidores de informes

Desde el servidor de almacenamiento remoto, genere un par de claves RSA como el usuario caelmservice y a continuación copie la clave pública con el nombre `authorized_keys_RSS` en el directorio `/tmp` de un servidor de informes CA Enterprise Log Manager. El servidor de informes habitualmente tiene un archivo `authorized_keys` en el directorio `.ssh` que contiene una concatenación de claves públicas de varios servidores de recopilación. Envíe la clave con un nombre único para que se pueda anexar al archivo `authorized_keys` ya existente.

Para generar un par de claves pública/privada RSA y copiar la clave pública del almacenamiento remoto en el servidor de informes

1. Inicie sesión en el servidor de almacenamiento remoto a través de `ssh` como el usuario `caelmadmin`.
2. Cambie los usuarios a `root`.
3. Cambie los usuarios a la cuenta de `caelmservice`.
`su - caelmservice`
4. Genere un par de claves RSA como usuario `caelmservice`.
`ssh-keygen -t rsa`
5. Pulse Intro para aceptar los valores predeterminados cuando aparezcan las siguientes solicitudes:
 - Introduzca el archivo donde se guardará la clave (`/opt/CA/LogManager/.ssh/id_rsa`):
 - Introduzca la frase de contraseña (queda vacío si no se utiliza frase de contraseña):
 - Introduzca de nuevo la misma frase de contraseña:
6. Cambie los permisos del directorio `.ssh` utilizando el siguiente comando.
`chmod 755 .ssh`
7. Desplácese hasta el directorio `.ssh`.
8. Copie `id_rsa.pub` con el nombre `authorized_keys_RSS` en el directorio `/tmp` del servidor de informes.
`scp id_rsa.pub caelmadmin@<reporting_server>:/tmp/authorized_keys_RSS`

Actualización del archivo de clave pública existente

Se ha copiado la clave pública, `authorized_keys_RSS`, en el directorio `/tmp` del servidor de informes. A continuación se debe preparar el archivo de clave pública para su utilización. La preparación implica anexar `authorized_keys_RSS` al archivo `authorized_keys`. La propiedad y los permisos adecuados ya están establecidos en el archivo `authorized_keys` existente.

Para anexar `authorized_keys_RSS` al archivo `authorized_keys` y copiarlo en la ubicación correcta

1. Inicie sesión en el servidor de informes de CA Enterprise Log Manager a través de `ssh` como usuario `caelmadmin`.
2. Cambie los usuarios a `root`.
3. Modifique los directorios por el directorio `/tmp` que contiene `authorized_keys_RSS`.
4. Copie el archivo `authorized_keys` existente de `.ssh` al directorio actual, `/tmp`.

```
cp /opt/CA/LogManager/.ssh/authorized_keys .
```

5. Agregue los contenidos de la clave pública del servidor de almacenamiento remoto al archivo `authorized_keys` que contiene las claves públicas de los servidores de recopilación.

```
cat authorized_keys_RSS >> authorized_keys
```

6. Modifique los directorios a `/opt/CA/LogManager/.ssh`.
7. Copie el archivo `authorized_keys` de `/tmp` a `.ssh`, el directorio actual:

```
cp /tmp/authorized_keys .
```

Consulta del catálogo de archivado

Puede crear consultas para realizar búsquedas de bases de datos frías (almacenadas de forma remota) en el catálogo de archivos local mediante filtros rápidos o avanzados. Los resultados de las consultas pueden ayudarle a identificar los archivos de base de datos que necesita restaurar para llevar a cabo una investigación.

Para realizar consultas en el catálogo de archivos

1. Haga clic en la ficha Administración y en la subficha Gestión de archivos.
Aparecerá la lista de carpetas del Explorador de archivos.
2. Haga clic en la carpeta Consulta de archivos y recatalogación.
En el panel de detalles, aparece el cuadro de diálogo de consultas de archivos.
3. Seleccione o introduzca el período para la consulta.
4. Haga clic en Agregar filtro, seleccione una columna e introduzca el valor de búsqueda de la columna. Puede agregar varios filtros.
5. Seleccione Excluir para realizar consultas en todos los registros *excepto* en aquellos en los que haya introducido un valor.

Nota: Si crea un filtro que especifica una columna que *no* está en el catálogo, CA Enterprise Log Manager devuelve todas las bases de datos del rango de tiempo especificado en lugar de un conjunto vacío. No es necesario que conozca todas las columnas catalogadas para crear una consulta de archivos útil.

6. Haga clic (opcional) en la ficha Filtros avanzados para agregar filtros avanzados. Incluye la información del evento si la columna tiene la relación apropiada con el valor introducido. Seleccione una columna, seleccione un operador y, a continuación, seleccione o introduzca un valor. A continuación, se muestran descripciones de operadores:

Operadores relacionales

Igual a, Distinto de, Menor que, Mayor que, Menor o igual a, Mayor o igual a.

Como

Incluye la información del evento si la columna contiene un patrón que haga coincidir la entrada de texto con el carácter comodín, %. L% incluye valores que comienzan por L. %L% incluye valores que contienen L, excepto aquellos en los que la L sea el primer o el último carácter.

Not like

Incluye la información del evento si la columna no contiene el patrón especificado.

In set

Incluye la información del evento si la columna contiene uno o varios valores del conjunto entrecomillado introducido. Debe separar con comas los diferentes valores del conjunto.

Not in set

Incluye la información del evento si la columna contiene uno o varios valores del conjunto entrecomillado introducido. Debe separar con comas los diferentes valores del conjunto.

Matches

Incluye cualquier información del evento que coincida con uno o más de los caracteres introducidos, de manera que puede buscar por palabras clave.

Keyed

Incluye cualquier información del evento que se haya definido como valor clave durante la configuración del servidor de informes. Utilice valores de clave para definir la relevancia empresarial u otros grupos organizativos.

Not Keyed

Incluye cualquier información del evento que no se haya definido como valor clave durante la configuración del servidor de informes. Utilice valores de clave para definir la relevancia empresarial u otros grupos organizativos.

7. Haga clic en Consulta.

Aparecerán los resultados de consultas. Los archivos que contienen registros que coinciden con los criterios de la consulta se muestran en la ruta completa, relativa a \$IGW_LOC. A continuación, se muestran algunos ejemplos:

../..LogManager/data/archive/<databaseFilename>

<remoteHostname>-../..LogManager/data/archive/<databaseFilename>

Restauración de archivos almacenados de forma automática

Si copia archivos almacenados de un sistema de almacenamiento externo al servidor remoto configurado para el almacenamiento automático, puede restaurarlos mediante el script `restore-ca-elm.sh`. Esta alternativa es más aconsejable que el empleo manual de la utilidad `LMArchive`.

Para restaurar archivos almacenados de forma automática

1. Utilice las credenciales de `caelmadmin` para iniciar sesión en el servidor de CA Enterprise Log Manager que contiene el sistema de almacenamiento de registro de eventos en el que desea restaurar las bases de datos.

2. Al solicitársele, dirija a los usuarios a la raíz, es decir:

```
su - root
```

3. Cambie los directorios a `/opt/CA/SharedComponents/iTechnology` mediante el atajo siguiente:

```
cd $IGW_LOC
```

4. Cuando se le solicite, cambie a los usuarios a la cuenta `caelmservice`.

```
su - caelmservice
```

5. Ejecute el comando siguiente, donde *userid* y *pwd* son las credenciales de una cuenta de usuario de CA Enterprise Log Manager con la función Administrator.

```
restore-ca-elm.sh -euser userid -epasswd pwd -rhost hostname -ruser userid -rlocation path -files file1,file2,file3...
```

Nota: Para permitir que un usuario que no sea administrador ejecute el script shell `restore-ca-elm`, cree una función personalizada y una política personalizada. A continuación, los usuarios a los que asigne esta función personalizada podrán especificar sus credenciales para *userid* y *pwd*.

Más información:

[Script de restauración para restaurar bases de datos almacenadas](#) (en la página 214)

[Ejemplo: Permitir a un usuario que no es administrador gestionar acciones de almacenamiento](#) (en la página 121)

[Copia de seguridad y restauración de ACS](#) (en la página 199)

Script de restauración para restaurar bases de datos almacenadas

No puede realizar consultas ni crear informes de datos que se encuentre en una base de datos fría de un servidor de almacenamiento remoto. Para realizar una consulta o crear un informe con estos datos, se deben encontrar en un estado tibio de un servidor de CA Enterprise Log Manager. El script shell de restauración, `restore-ca-elm.sh`, es una utilidad de línea de comandos que desplaza una base de datos fría y su firma digital a un servidor de CA Enterprise Log Manager específico y la restaura a un estado tibio. La utilidad de restauración se puede utilizar para devolver una base de datos al servidor de informes original o a un punto de restauración dedicado. La configuración de la autenticación no interactiva es un requisito previo a la ejecución del script de restauración.

Ejecute el script de restauración desde el servidor de CA Enterprise Log Manager en el que desee restaurar los archivos. El host remoto identificado en el comando hace referencia al servidor de almacenamiento remoto. Las bases de datos frías se encuentran en el directorio de archivado del servidor de almacenamiento remoto.

Los requisitos para restaurar los archivos de bases de datos en el servidor de informes original o en un servidor de punto de restauración son los siguientes:

- La propiedad de archivo clave de RSA se haya establecido en el servidor remoto.
- Se haya concedido permiso para la carpeta `/opt/CA/LogManager` a `caelmservice` en el servidor remoto.

Si restaura archivos en un servidor de punto de restauración, deberá llevar a cabo las siguientes acciones adicionales:

1. Copie la clave de RSA del servidor de almacenamiento remoto al servidor del punto de restauración.
2. Defina la propiedad del archivo de claves de RSA en el servidor del punto de restauración.

El comando tiene el formato siguiente:

```
restore-ca-elm.sh -euser userid -epasswd pwd -rhost hostname -ruser userid -  
rlocation path -files file1,file2,file3...
```

-euser *username*

Especifica el nombre de usuario de una cuenta de usuario de CA Enterprise Log Manager con el rol Administrator.

-epasswd *pwd*

Especifica la contraseña de CA Enterprise Log Manager asociada al nombre del usuario.

-rhost *host*

Especifica el nombre de host o la dirección IP del host remoto en el que se encuentran los archivos de la base de datos fría en el directorio de archivado. El host remoto no es un servidor de CA Enterprise Log Manager.

-ruser *remote user*

Especifica la cuenta de usuario con permisos para la ruta /opt/CA/LogManager y la propiedad de la carpeta .ssh que contiene el archivo de claves autorizadas. Generalmente, ésta es la cuenta de usuario de caelmservice.

-rlocation *path*

Especifica la ruta a los archivos de base de datos en el servidor de almacenamiento remoto. Si el servidor de almacenamiento remoto es un servidor UNIX, la ruta será /opt/CA/LogManager/data/archive.

files *file1,file2,file3...*

Especifica una lista separada por comas, sin espacios, de los archivos de la base de datos que desea restaurar.

Ejemplo: Restaurar scripts shell

El ejemplo de comando siguiente se ejecuta desde el servidor de CA Enterprise Log Manager en el que se desean restaurar los archivos de la base de datos archivada. Dicho comando lo ejecuta un usuario con credenciales de cuenta Administrator1, calm_r12. El servidor remoto al que se han trasladado las bases de datos almacenadas desde el almacenamiento externo se denomina NY-Almacenamiento-Svr. Este servidor remoto se ha configurado mediante una cuenta caelmservice que tiene la propiedad de la carpeta .ssh en la que se ha copiado la clave pública RSA. Esta cuenta también tiene privilegios completos en la estructura de directorio /opt/CA/LogManager. Este comando especifica que los archivos que se van a restaurar están en la ruta del directorio de datos/archivo del servidor NY-Storage-Svr e identifica el archivo de la base de datos que se desea restaurar como NY-Storage-Svr_20081206192014.db.cerod.

```
restore-ca-elm.sh -euser Administrator1 -epasswd calm_r12 -rhost NY-Storage-Svr -
ruser caelmservice -rlocation /opt/CA/LogManager/data/archive -files
NY-Storage-Svr_20081206192014.db.cerod
```

Más información:

[Restauración de archivos almacenados de forma automática](#) (en la página 213)

[Configuración de autenticaciones no interactivas para su restauración](#) (en la página 204)

[Ejemplo: configuración de la autenticación desde un servidor de almacenamiento remoto a un servidor de punto de restauración](#) (en la página 205)

[Ejemplo: configuración de la autenticación de un servidor de almacenamiento a un servidor de informes](#) (en la página 208)

Copia de seguridad manual de bases de datos archivadas

CA Enterprise Log Manager crea de forma automática una nueva base de datos archivada cada vez que se desplazan datos del almacenamiento caliente al tibio, según lo detecte la configuración que haya realizado. Aunque se recomienda configurar el almacenamiento automático para desplazar las bases de datos tibias a un servidor remoto, puede emplear sus propias herramientas para realizar copias de seguridad de las bases de datos archivadas y, a continuación, ejecutar la utilidad LMArchive para notificar al sistema que ha realizado la copia de seguridad.

Se recomienda que realice copias de seguridad de las bases de datos tibias a diario, a través del método automatizado o el método manual descritos aquí. Esto es importante, ya que los archivos de almacenamiento tibio se eliminan de forma automática tras el período de tiempo especificado o cuando el espacio en el disco alcanza el porcentaje indicado.

La realización de copias de seguridad de bases de datos tibias de forma manual consta de los pasos siguientes:

1. Identifique las bases de datos tibias que aún no posean copias de seguridad.
2. Realice las copias de seguridad.
3. Registre las copias de seguridad.

Más información

[Identificación de bases de datos que no tienen copia de seguridad](#) (en la página 217)

[Realización de copias de seguridad](#) (en la página 219)

[Registro de las copias de seguridad](#) (en la página 219)

Identificación de bases de datos que no tienen copia de seguridad

Puede ver una lista de las bases de datos archivadas que aún no posean una copia de seguridad mediante la utilidad LMArchive. La capacidad de obtener resultados fiables supone que alguien ejecute esta utilidad con la opción *-notify arch* cada vez que se realice una copia de seguridad de las bases de datos archivadas.

Importante: para evitar confusiones, manténgase al día en cuanto a las notificaciones enviadas a CA Enterprise Log Manager sobre las copias de seguridad realizadas.

Para mostrar los nombres de todos los archivos de bases de datos archivadas actuales que no poseen copias de seguridad

1. Utilice las credenciales **caelmadmin** para iniciar sesión en el servidor de CA Enterprise Log Manager con el sistema de almacenamiento de registro de eventos que contiene las bases de datos cuya copia de seguridad debe realizar para su archivo.
2. Al solicitársele, dirija a los usuarios a la raíz, es decir:

`su - root`
3. Cambie los directorios a `/opt/CA/SharedComponents/iTechnology` mediante el atajo siguiente:

`cd $IGW_LOC`
4. Ejecute el comando siguiente, donde *username* y *pwd* son las credenciales de una cuenta de usuario de CA Enterprise Log Manager con el rol Administrator.

```
LMArchive -euser username -epassword pwd -list inc
```

Ejemplo: Mostrar todos los archivos guardados en CA Enterprise Log Manager actuales que no posean copia de seguridad

El comando siguiente emitido por un administrador solicita una lista de todas las bases de datos tibias que no posean copia de seguridad.

```
LMArchive -euser Administrator1 -epassword calmr12 -list inc
```

Aparece una lista de archivos de almacenamiento que no poseen copia de seguridad. Dicha lista tiene un formato parecido al siguiente:

```
CAELM Archived Files (not backed up):  
  calm04_20091206192014.db.cerod  
  calm04_20091206192014.db.sig
```

Realización de copias de seguridad

Si no ha configurado el archivo automático de un servidor de informes de CA Enterprise Log Manager a un servidor de almacenamiento remoto que no es un servidor de CA Enterprise Log Manager, debe realizar una copia de seguridad manual de las bases de datos archivadas y trasladarlas a una ubicación de almacenamiento segura, como un disco o un servidor independiente.

Importante: Asegúrese de realizar una copia de seguridad de las bases de datos y de trasladarlas antes de *eliminarlas* del servidor de informes de CA Enterprise Log Manager.

Las bases de datos tibias se eliminan de forma automática cuando se alcanza el valor configurado del número máximo de días archivado, o cuando el porcentaje de espacio en el disco es inferior al valor configurado del espacio en disco para archivo. Para evitar pérdidas de datos por los archivos eliminados, realice copias de seguridad de forma periódica.

Para realizar copias de seguridad de bases de datos tibias de forma manual

1. Utilice las credenciales caelmadmin para iniciar sesión en el servidor de informes de CA Enterprise Log Manager con el sistema de almacenamiento de registro de eventos que contiene las bases de datos de destino.
2. Dirija a los usuarios a la raíz, es decir:

```
su - root
```
3. Cambie los directorios a /opt/CA/LogManager/data/archive.
4. Realice una copia de seguridad de las bases de datos con la herramienta de copia de seguridad que seleccione y trasládelas a un servidor de almacenamiento interno del emplazamiento o a una ubicación externa para un almacenamiento durante largo tiempo, según los procedimientos del emplazamiento.

Registro de las copias de seguridad

Cada vez que realice la copia de seguridad de una o más bases de datos almacenadas, asegúrese de que registra esta acción en el equipo de CA Enterprise Log Manager del que realizó la copia de seguridad.

Nota: Si no registra cada copia de seguridad, se enviarán datos incorrectos al emplear la utilidad LMArchive para obtener una lista de las bases de datos con copia de seguridad.

Para registrar las copias de seguridad de determinadas bases de datos almacenadas

1. Utilice las credenciales caelmadmin para iniciar sesión en el servidor de CA Enterprise Log Manager con el sistema de almacenamiento de registro de eventos que contiene las bases de datos cuya copia de seguridad ha realizado.
2. Al solicitársele, dirija a los usuarios a la raíz, es decir:

`su - root`
3. Cambie los directorios a /opt/CA/SharedComponents/iTechnology mediante el atajo siguiente:

`cd $IGW_LOC`
4. Ejecute el comando siguiente, donde *username* y *pwd* son las credenciales de una cuenta de usuario de CA Enterprise Log Manager con la función Administrator.

```
LMArchive -euser username -epassword pwd -notify arch -files  
file1,file2,file3...
```

Ejemplo: Informar a CA Enterprise Log Manager de que determinados archivos poseen copia de seguridad

El comando siguiente, emitido por el administrador llamado Administrator1, informa al sistema de almacenamiento de registro de eventos de CA Enterprise Log Manager de que se ha realizado una copia de seguridad de la base de datos tibia, calm04_20091206192014.db.cerod. Las bases de datos con copias de seguridad se pueden trasladar de forma manual a un sistema de almacenamiento externo para guardarlas durante largo tiempo.

```
LMArchive -euser Administrator1 -epassword calmr12 -notify arch  
-files calm04_20091206192014.db.cerod
```

Aparece la notificación del archivo de almacenamiento. Dicha notificación tiene un formato parecido al siguiente:

```
Notificación de archivado enviada para el archivo  
calm04_20091206192014.db.cerod...
```

Restauración manual de archivos en el sistema de almacenamiento de registro de eventos original

En ocasiones, puede necesitar restaurar archivos de bases de datos frías para realizar consultas o informes en el directorio de archivo de un servidor de CA Enterprise Log Manager. Esto puede resultar necesario para investigar un problema de seguridad o para realizar una auditoría de conformidad anual o semestral. Los procedimientos empleados dependen de estos dos factores:

- Si ha empleado el archivo automático para realizar la copia de seguridad de los archivos que desea restaurar
- Si restaura los archivos en el servidor de informes original o en un servidor diferente, como un servidor de punto de restauración especializado

Si desea realizar la restauración en un servidor diferente, consulte "Restauración de archivos en un sistema de almacenamiento de registro de eventos nuevo".

Cuando restaure archivos en el servidor de informes original, siga estos procedimientos:

1. Prepare la restauración de las bases de datos archivadas mediante la identificación de archivos que desea restaurar y la determinación del directorio de archivo.
2. Traslade las bases de datos del almacenamiento externo al directorio de archivo de la ubicación del servidor remoto que haya configurado para el archivo automático o al servidor de informes original.
3. Si ha trasladado los archivos almacenados al servidor de almacenamiento remoto configurado para el archivo automático, inicie sesión en el CA Enterprise Log Manager de informes y restaure los archivos almacenados automáticamente desde el servidor de almacenamiento remoto mediante el script `restore-ca-elm.sh`.
4. Si ha trasladado los archivos almacenados al directorio de archivo del servidor de CA Enterprise Log Manager de informes original, restaure los archivos almacenados de forma manual mediante la utilidad `LMArchive`.
5. Compruebe que la base de datos descongelada puede recibir consultas: ejecute una consulta con la fecha de finalización establecida en la fecha de la base de datos restaurada y analice los resultados de dicha consulta.

Más información

[Preparación para restaurar bases de datos almacenadas](#) (en la página 223)

[Desplazamiento de bases de datos archivadas a un directorio de archivo](#) (en la página 225)

[Restauración de archivos almacenados de forma automática](#) (en la página 213)

[Restauración de archivos almacenados de forma manual](#) (en la página 226)

[Verificación de la restauración](#) (en la página 228)

Preparación para restaurar bases de datos almacenadas

Antes de restaurar bases de datos almacenadas, debe conocer los datos siguientes:

- Los nombres de los archivos que desea restaurar.
- La ruta del directorio de archivo en el que se van a copiar los archivos recuperados del almacenamiento externo. La ruta es siempre `/opt/CA/LogManager/data/archive`.

Puede realizar consultas en el catálogo de archivos mediante la ficha de administración de CA Enterprise Log Manager, Explorador de recopilación de registros, donde puede especificar filtros simples o avanzados. También puede emplear la utilidad de línea de comandos como se describe aquí.

Si ya tiene a mano la información necesaria, omita este procedimiento.

Para preparar la restauración de bases de datos almacenadas

1. Utilice las credenciales de caelmadmin para iniciar sesión en el servidor de CA Enterprise Log Manager que contiene el sistema de almacenamiento de registro de eventos en el que desea restaurar las bases de datos.

2. Al solicitársele, dirija a los usuarios a la raíz, es decir:

```
su - root
```

3. Cambie los directorios a `/opt/CA/SharedComponents/iTechnology` mediante el atajo siguiente:

```
cd $IGW_LOC
```

4. Identifique las bases de datos que desea restaurar en una lista de archivos que incluye aquellos que tienen copias de seguridad y se han trasladado a un sistema de almacenamiento externo. Para ver una lista de todos los archivos guardados en este catálogo de archivos, ejecute el comando siguiente, donde `userid` y `pwd` son las credenciales de una cuenta de usuario de CA Enterprise Log Manager con el rol Administrator.

```
LMArchive -euser userid -epassword pwd -list all
```

Aparece una lista con todos los archivos guardados.

5. (Opcional) Si la restauración se realiza a partir de copias de seguridad manuales, determine la ubicación del directorio de archivos en el que desea copiar los archivos guardados en estado frío que se han identificado. Ejecute el comando siguiente, donde `userid` y `pwd` son las credenciales de una cuenta de usuario de CA Enterprise Log Manager con el rol Administrator.

```
LMArchive -euser userid -epassword pwd -list loc
```

Aparece el directorio de archivos.

Ejemplo: Mostrar todos los archivos de almacenamiento de CA Enterprise Log Manager actuales

El comando siguiente emitido por el administrador de CA Enterprise Log Manager, Administrator1, solicita una lista de todas las bases de datos ubicadas en el directorio de archivos del sistema de almacenamiento de registro de eventos.

```
LMArchive -euser Administrator1 -epassword calmr12 -list all
```

Aparece una lista de los archivos de almacenamiento actuales con un formato similar al siguiente:

```
CAELM Archived Files:
  calm04_20091206191941.db.cerod
  calm04_20091206191958.db.cerod
  calm04_20091206192014.db.cerod
  calm04_20091206191941.db.sig
  calm04_20091206191958.db.sig
  calm04_20091206192014.db.sig
```

Ejemplo: Mostrar el directorio de archivos de CA Enterprise Log Manager

El comando siguiente, emitido por un administrador de CA Enterprise Log Manager, Administrator1, solicita la ubicación del directorio de las bases de datos almacenadas:

```
LMArchive -euser Administrator1 -epassword calmr12 -list loc
```

A continuación, se muestra una respuesta habitual:

```
CAELM Archive Location (localhost):
../LogManager/data/archive
```

Más información:

[Consulta del catálogo de archivado](#) (en la página 211)

Desplazamiento de bases de datos archivadas a un directorio de archivo

Si ha trasladado los archivos almacenados a una ubicación externa, utilice los procedimientos de su emplazamiento para recuperarlos y devolverlos a la ubicación interna.

Traslade las bases de datos de vuelta al directorio de archivo del servidor de CA Enterprise Log Manager original o a un servidor remoto configurado para una autenticación no interactiva. El directorio de archivo es `/opt/ca/LogManager/data/archive`.

Para trasladar una base de datos archivada desde un almacenamiento externo a su red

1. Desplace los archivos de la base de datos que desee restaurar desde el almacenamiento externo hasta su red a través de uno de los métodos siguientes:
 - Si emplea el archivo automático para trasladar automáticamente los archivos almacenados al servidor remoto, cópielos de nuevo en el directorio de archivo de dicho servidor remoto. (Este servidor remoto ya está configurado para una autenticación no interactiva con el servidor de CA Enterprise Log Manager en el que se restaurarán las bases de datos archivadas.)
 - Si no utiliza el archivo automático, copie de nuevo los archivos almacenados en el directorio de archivo del servidor de CA Enterprise Log Manager original.
2. Siga uno de los métodos indicados a continuación en función de la ubicación de los archivos almacenados.
 - Si los archivos almacenados están en el servidor remoto configurado para realizar un archivo automático, restaure los archivos almacenados de forma automática mediante el script `restore-ca-elm.sh`.
 - Si los archivos almacenados están en el directorio de archivo del servidor de CA Enterprise Log Manager original, informe a CA Enterprise Log Manager de que los archivos almacenados se han restaurado mediante la utilidad `LMArchive`. Tras una notificación, los archivos restaurados adoptan un estado descongelado.

Más información:

[Restauración de archivos almacenados de forma automática](#) (en la página 213)
[Restauración de archivos almacenados de forma manual](#) (en la página 226)

Restauración de archivos almacenados de forma manual

Tras haber restaurado una o más bases de datos del almacenamiento a largo plazo al directorio de archivo, debe modificar la pertenencia del directorio de archivo para asignarla al usuario caelmservice antes de notificar a CA Enterprise Log Manager que las bases de datos se han restaurado mediante la utilidad LMArchive. La utilidad LMArchive no reconoce los archivos almacenados pertenecientes a la raíz.

La ejecución de LMArchive con la opción `-notify rest` modifica el estado de los archivos de la base de datos almacenada de frío a descongelado, de manera que se pueden emplear para consultas e informes.

Los administradores configuran el número de horas durante las que se retiene una base de datos archivada descongelada antes de eliminarse automáticamente del directorio archivado mediante el ajuste Política de exportación de la configuración de servicios del sistema de almacenamiento de registro de eventos.

Para restaurar manualmente archivos de bases de datos archivadas

1. Utilice las credenciales **caelmadmin** para iniciar sesión en el servidor de CA Enterprise Log Manager con el sistema de almacenamiento de registro de eventos que contiene las bases de datos restauradas.

2. Al solicitársele, dirija a los usuarios a la raíz, es decir:

```
su - root
```

3. Cambie los directorios por el directorio `/data`. Por ejemplo:

```
cd /opt/CA/LogManager/data
```

4. Asigne la propiedad del directorio de archivo (`/opt/CA/LogManager/data/archive`) a la cuenta caelmservice.

```
chown -R caelmservice:caelmservice archive
```

La propiedad de los archivos de almacenamiento cambia a caelmservice, el usuario del sistema operativo interno, que es una cuenta sin inicio de sesión.

5. Cambie los directorios a `/opt/CA/SharedComponents/iTechnology` mediante el atajo siguiente:

```
cd $IGW_LOC
```

6. Ejecute el comando siguiente, donde *username* y *pwd* son las credenciales de una cuenta de usuario de CA Enterprise Log Manager con la función Administrator.

```
LMArchive -euser username -epassword pwd -notify rest -files  
file1,file2,file3
```

Aparece una confirmación de restauración. CA Enterprise Log Manager descongela los archivos indicados. Los archivos descongelados se retienen durante el número de horas especificado; puede configurar la retención durante un máximo de siete días.

Nota: Ahora, podrá ejecutar consultas e informes con los datos de eventos incluidos en los archivos almacenados restaurados.

Ejemplo: Notificar a CA Enterprise Log Manager de que se han restaurado determinadas bases de datos

El comando siguiente, emitido por un usuario de CA Enterprise Log Manager con la función Administrator, notifica al sistema de almacenamiento de registro de eventos de CA Enterprise Log Manager que la base de datos fría especificada, *calm04_20091206192014.db*, se ha copiado en el directorio de archivo.

```
LMArchive -euser Administrator1 -epassword calmr12 -notify rest  
-files calm04_20091206192014.db.cerod
```

Aparece una confirmación de restauración con un formato parecido al siguiente:

```
Notificación de restauración enviada para el archivo  
calm04_20091206192014.db.cerod
```

Verificación de la restauración

Puede comprobar rápidamente si la base de datos restaurada está disponible para su examen mediante la ejecución de una consulta rápida. Las consultas normales muestran datos de las bases de datos restauradas en estado tibio y descongelado.

Observe el proceso siguiente.

1. Copie una consulta de suscripción realizada para visualizar el tipo de detalles del evento que contiene la base de datos restaurada.
2. Vaya al paso del asistente de diseño de consultas en el que se definen las condiciones del resultado e introduzca un rango de fechas que corresponda a los archivos de la base de datos recién descongelada.
3. Guarde la consulta.
4. Ejecute la consulta.

Restauración manual de archivos en sistemas de almacenamiento de registro de eventos nuevos

Es posible que necesite restaurar archivos almacenados fríos para realizar consultas o informes, como para una auditoría de conformidad semestral o anual. Si designa un CA Enterprise Log Manager para que actúe como punto de restauración para las investigaciones en datos fríos, debe forzar una reconstrucción del catálogo cada vez que restaura una base de datos nueva en dicho CA Enterprise Log Manager. La reconstrucción del catálogo, o recatalogación, sólo es necesaria al restaurar datos en un servidor distinto de aquél en el que se han generado.

Importante: Asegúrese de que el ajuste Número máximo de días de archivado del sistema de almacenamiento de registro de eventos de este servidor sea el adecuado. Si no es así, los archivos restaurados se eliminarán de forma inmediata.

La recatalogación se lleva a cabo de manera automática al reiniciar iGateway si es necesario. Si las bases de datos no se catalogaron por completo antes de apagar iGateway, el proceso de recatalogación finaliza al reiniciar iGateway. Si añade una o varias bases de datos al directorio de bases de datos de archivo mientras iGateway está apagado, el proceso de recatalogación se llevará a cabo en el siguiente inicio de iGateway.

La restauración de archivos almacenados desde un sistema de almacenamiento externo a un CA Enterprise Log Manager diferente de aquél desde el que se hicieron las copias de seguridad consta de los pasos siguientes:

1. Identificación de las bases de datos que desea restaurar. Para obtener ayuda, consulte el catálogo de archivos con filtros.
2. Desplazamiento de los archivos de almacenamiento fríos identificados de un almacén externo a la red.
3. Copia de las bases de datos desplazadas al directorio de archivo. Para mostrar el directorio de archivo, ejecute la utilidad LMArchive con la opción -list loc.
4. Reconstrucción del catálogo de archivos (recatalogación).

La reconstrucción del catálogo de archivos para agregar una única base de datos puede llevar varias horas. Tras esperar lo necesario para que finalice el proceso de recatalogación, puede comenzar la investigación mediante la ejecución de consultas e informes en los registros de eventos de las bases de datos restauradas.

5. Verifique la restauración mediante la emisión de una consulta.

Nota: Si define un CA Enterprise Log Manager como punto de restauración, asegúrese de excluirlo de la federación.

Más información:

[Desplazamiento de bases de datos archivadas a un directorio de archivo](#) (en la página 225)

[Configuración del número máximo de días de archivado para los archivos restaurados](#) (en la página 230)

[Adición de bases de datos restauradas al catálogo](#) (en la página 231)

[Verificación de la restauración](#) (en la página 228)

[Ejemplo: Permitir a un usuario que no es administrador gestionar acciones de almacenamiento](#) (en la página 121)

Configuración del número máximo de días de archivado para los archivos restaurados

Al configurar el sistema de almacenamiento de registro de eventos de un servidor de CA Enterprise Log Manager establecido como punto de restauración, es recomendable que anule la configuración global de Número máximo de días de archivado y la establezca al máximo: 28.000. Si el número de días durante los que se guardan los archivos de las bases de datos almacenadas antes de eliminarlos se establece a un valor inferior al de la antigüedad de los archivos de las bases de datos restauradas, el sistema elimina dichos archivos inmediatamente tras haberlos restaurado a un estado tibio.

Nota: Este procedimiento sólo se aplica a los archivos restaurados en un sistema de almacenamiento de registro de eventos nuevo.

Para establecer el número máximo de días según la antigüedad de los archivos restaurados

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. En la lista de servicios, expanda la carpeta Almacenamiento de registro de eventos y seleccione el servidor de CA Enterprise Log Manager que se haya definido como punto de restauración.
3. Haga clic en el botón de alternar situado junto a Número máximo de días de archivado para cambiar a la configuración local y activar el campo de entrada.
4. Establezca el valor del campo en un número de días que se adapte al archivo más antiguo de los que va a restaurar. El valor máximo es 28.000.
5. Haga clic en Guardar.

Adición de bases de datos restauradas al catálogo

Si copia la base de datos restaurada directamente en el directorio de archivo de un servidor distinto de aquél en el que se haya generado, deberá volver a crear el catálogo de archivos para agregar la base de datos restaurada.

No emplee la recatalogación en ninguno de los casos siguientes:

- Si utiliza el script `restore-ca-elm.sh` para restaurar una base de datos almacenada, ya que el script shell de restauración realiza la recatalogación por usted.
- Si copia la base de datos restaurada directamente en el directorio de archivo del mismo servidor en el que se generó y, a continuación, indica a CA Enterprise Log Manager que se ha restaurado la base de datos mediante la opción `-notify rest` de LMArchive.

El proceso de recatalogación establece que la base de datos restaurada está en estado "tibio", y no "descongelado", como ocurre con la opción `-notify rest` de LMArchive. Por lo tanto, sigue las reglas de archivo normales en lugar de la política de exportación establecida en la configuración del sistema de almacenamiento de registro de eventos.

Para volver a crear el catálogo de archivos para añadir la base de datos restaurada

1. Haga clic en la ficha Administración y en la subficha Gestión de archivos.
Aparecerá la lista de carpetas de la Gestión de archivos.
2. Haga clic en la carpeta Consulta de archivos y recatalogación.
Tres botones, incluido Recatalogar, aparecen sobre las fichas de Filtros rápidos y Filtros avanzados.
3. Haga clic en Recatalogar.
Aparece un mensaje de confirmación de acción correcta. La base de datos restaurada se añade al catálogo en estado tibio.

Más información:

[Ejemplo: Permitir a un usuario que no es administrador gestionar acciones de almacenamiento](#) (en la página 121)

Seguimiento de copia de seguridad/restauración de LMArchive

LMArchive es la utilidad de línea de comandos que realiza el seguimiento de la copia de seguridad y la restauración de bases de datos tibias en el almacén de registro de eventos de un servidor de CA Enterprise Log Manager. Utilice *LMArchive* para realizar consultas de la lista de archivos de bases de datos tibias que están listos para su almacenamiento. Tras realizar una copia de seguridad de la base de datos listada y trasladarla al almacenamiento a largo plazo (frío), utilice *LMArchive* para crear un registro en el servidor de CA Enterprise Log Manager en el que se realizó la copia de seguridad de dicha base de datos. Tras restaurar la base de datos fría en su servidor de CA Enterprise Log Manager original, utilice *LMArchive* para notificar a CA Enterprise Log Manager, quien, a su vez, descongela los archivos de la base de datos fría para que, una vez descongelados, se puedan emplear en las consultas.

El comando tiene el formato siguiente:

```
LMArchive -euser username -epassword pwd {-list [loc|all|inc] | -notify  
[arch|rest] -files file1,file2,file3...}
```

-euser *username*

Especifica el nombre de usuario de una cuenta de usuario de CA Enterprise Log Manager con la función Administrator.

-epassword *pwd*

Especifica la contraseña de CA Enterprise Log Manager asociada al nombre del usuario.

-list [loc | all | inc]

Solicita una lista de uno de los elementos siguientes: las ubicaciones del directorio de archivo, los nombres de todas las bases de datos tibias y frías, los nombres de las bases de datos tibias únicamente

loc

Solicita la ubicación del directorio de archivo.

all

Solicita una lista de todos los nombres de archivos ubicados en el directorio de archivo del almacén de registro de eventos.

inc

Solicita una lista incremental de los archivos de bases de datos tibias que no se hayan archivado. La solicitud devuelve los nombres de aquellos archivos de los que no se haya realizado una copia de seguridad, se hayan desplazado a un medio de almacenamiento externo o cuyo estado se haya cambiado a frío. El estado de los archivos cambia a frío cuando se notifica el movimiento a través del comando de notificación de esta utilidad.

-notify [arch | rest]

Informa al sistema de almacenamiento de registro de eventos de CA Enterprise Log Manager de que los archivos especificados se han copiado o restaurado de forma correcta.

arch

Informa al sistema de almacenamiento de registro de eventos de CA Enterprise Log Manager de que los archivos especificados se han copiado de forma correcta.

rest

Informa al sistema de almacenamiento de registro de eventos de CA Enterprise Log Manager de que los archivos especificados se han restaurado de forma correcta.

-files *file1,file2,file3...*

Especifica los nombres de los archivos de base de datos que han copiado o restaurado.

Más información:

[Acerca del almacenamiento de registros](#) (en la página 194)

[Identificación de bases de datos que no tienen copia de seguridad](#) (en la página 217)

[Registro de las copias de seguridad](#) (en la página 219)

[Preparación para restaurar bases de datos almacenadas](#) (en la página 223)

[Restauración de archivos almacenados de forma manual](#) (en la página 226)

Capítulo 7: Suscripción

Esta sección contiene los siguientes temas:

[Actualización a la versión 12.5 de CA Enterprise Log Manager mediante suscripción](#) (en la página 235)

[Consulta del estado de suscripción global](#) (en la página 237)

[Consulte el estado de suscripción de un servidor](#) (en la página 238)

[Edición de la configuración de suscripción global](#) (en la página 240)

[Edición de la configuración de suscripción local de los servidores](#) (en la página 241)

[Descarga y selección de módulos para la suscripción sin conexión](#) (en la página 243)

[Acerca de las actualizaciones a petición](#) (en la página 245)

[Espacio libre en disco para actualizaciones](#) (en la página 249)

[Acerca de las claves públicas de suscripción](#) (en la página 250)

[Eventos autocontrolados para suscripción](#) (en la página 250)

[Aplicación de actualizaciones de suscripción a agentes y conectores](#) (en la página 255)

Actualización a la versión 12.5 de CA Enterprise Log Manager mediante suscripción

Para actualizar CA Enterprise Log Manager a la versión 12.5, actualice primero a la versión 12.5 del producto Log Manager, a continuación actualice el resto de módulos de CA Enterprise Log Manager, como los módulos Contenido, Integración y Agente. Todas las tareas de actualización se realizan mediante la suscripción.

Importante: Actualice el servidor de CA Enterprise Log Manager de gestión antes de instalar cualquier servidor nuevo de CA Enterprise Log Manager en la red. De ese modo se permite el registro adecuado de los servidores nuevos.

Para actualizar a la versión de 12.5 de CA Enterprise Log Manager

1. Actualice la versión del gestor de registro a la versión de 12.5.

Nota: La interfaz del usuario de CA Enterprise Log Manager 12.5 actualizada clasifica tanto el módulo de suscripción como el servicio de suscripción en la ficha Administración, y la subficha Servicios. El módulo de suscripción refleja la interfaz y la funcionalidad anterior a la actualización a la versión 12.5, y está presente para asegurarle una comunicación correcta entre todos los servidores de CA Enterprise Log Manager durante la actualización a la versión 12.5. Una vez que haya actualizado el gestor de registro a la versión 12.5 en un servidor de CA Enterprise Log Manager determinado, utilice únicamente el servicio de suscripción para realizar más tareas de suscripción y cambios de configuración.

2. Actualice el resto de módulos de CA Enterprise Log Manager.

Importante: Después de haber realizado el paso 1, la interfaz de usuario de CA Enterprise Log Manager 12.5 actualizada enumera tanto el módulo de suscripción como el servicio de suscripción. Utilice únicamente el servicio de suscripción, y no el módulo de suscripción, para realizar el resto de suscripciones, incluido este paso. El módulo de suscripción está presente solamente para ayudar a asegurarle una comunicación correcta entre todos los servidores de CA Enterprise Log Manager durante la actualización a la versión 12.5; no lo utilice para realizar funciones de suscripción posteriores a la actualización.

3. Si los módulos Agente o Conector se encontraban entre las actualizaciones, instale agentes o conectores actualizados.
4. Vuelva a registrar los productos de terceros y otros productos de CA, como CA Access Control, que muestra los informes de CA Enterprise Log Manager en las interfaces nativas mediante las llamadas a API abierta.

Con este paso se actualizan los certificados que cambiaron en esta versión. Para obtener más información, consulte la *Guía de programación de la API de CA Enterprise Log Manager*.

Nota: Para obtener información detallada sobre la realización de estos pasos, consulte *Actualización a la versión 12.5 de CA Enterprise Log Manager mediante suscripción* en las *Notas de la versión 12.5 de CA Enterprise Log Manager*. Consulte también las notas de la versión para cualquier problema conocido relacionado con las actualizaciones de suscripción.

Más información:

[Aplicación de actualizaciones de suscripción a agentes y conectores](#) (en la página 255)

Consulta del estado de suscripción global

El servicio de suscripción descarga y distribuye módulos de suscripción seleccionados a los servidores de CA Enterprise Log Manager según una programación configurada o según una actualización a petición. Se puede consultar el estado de suscripción actual de los servidores de CA Enterprise Log Manager a través del cuadro de mandos de la suscripción.

El cuadro de mandos de la suscripción muestra el progreso de cualquier actualización que se encuentre en proceso de descarga o instalación en un servidor de CA Enterprise Log Manager. También se puede consultar el estado de cualquier actualización del contenido actualmente en curso y una lista de todas las actualizaciones del contenido instaladas previamente.

Consultar el estado global de las suscripciones

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Haga clic en Servicio de suscripción.
Aparecerá la configuración del servicio global para el servicio de suscripción, con la ficha Cuadro de mandos de la suscripción seleccionada.
3. Para consultar el estado de las actualizaciones del contenido, examine la ventana Estado de la suscripción del contenido.
Si hay alguna actualización de contenido actualmente en curso, el estado de la actualización se indicará mediante una barra de progreso y mensajes de estado. Haga clic en el botón Actualizar para mostrar el progreso más reciente de la actualización.
4. Para consultar una lista de todas las actualizaciones del contenido instaladas hasta la fecha, haga clic en Explorar catálogo.
Aparecerá la ventana Contenido. Haga clic en un tipo de contenido para mostrar el nombre, la fecha y la versión de todas las actualizaciones asociadas que se hayan instalado hasta la fecha.
5. Para consultar el estado de suscripción de cualquier servidor de CA Enterprise Log Manager, examine la ventana Servidores.
Si hay alguna actualización en curso en cualquier servidor de CA Enterprise Log Manager, aparecerá una barra de progreso en la columna Progreso de ese servidor. Haga clic en el botón Actualizar para mostrar el progreso más reciente de la actualización.
La ventana Servidores también muestra información sobre cada servidor de CA Enterprise Log Manager, incluido lo siguiente:

Estado

Muestra el estado de la suscripción de un servidor de CA Enterprise Log Manager dado. Los estados de suscripción son Inactivo, En espera, Descargando, Instalando, Completado y Erróneo.

Mensaje

Muestra cualquier mensaje relacionado con el estado de suscripción de un servidor de CA Enterprise Log Manager dado.

Fecha

Muestra la fecha de la última acción de actualización de un servidor de CA Enterprise Log Manager dado.

Consulte el estado de suscripción de un servidor

El servicio de suscripción descarga y distribuye módulos de suscripción seleccionados a los servidores de CA Enterprise Log Manager según una programación configurada o según una actualización a petición. Se puede consultar el estado de suscripción actual de un servidor de CA Enterprise Log Manager específico a través del cuadro de mandos de la suscripción global o a través de la ventana Estado local del servidor.

Cómo consultar el estado de suscripción de un servidor de CA Enterprise Log Manager

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Haga clic en Servicio de suscripción.

Aparecerá la configuración del servicio global para el servicio de suscripción, con la ficha Cuadro de mandos de la suscripción seleccionada.

3. A continuación, realice una de las siguientes acciones:

- En la ventana Servidores, examine la información de estado del servidor deseado. Si hay alguna actualización en curso, aparecerá una barra de progreso en la columna Progreso de ese servidor. Haga clic en el botón Actualizar para mostrar el progreso más reciente. La ventana Servidores también muestra información adicional sobre cada servidor de CA Enterprise Log Manager, incluidos Estado, Mensaje y Fecha.

o

- Para obtener información más detallada, en la ventana Servidores, haga clic en el nombre del servidor deseado para abrir la ventana Estado local de ese servidor. Si hay alguna actualización en curso, aparecerán una barra de progreso y mensajes de estado en la ventana Estado que indican el progreso de la actualización. Haga clic en el botón Actualizar para mostrar el progreso más reciente. La ventana Servidores también muestra información sobre cada servidor de CA Enterprise Log Manager, incluido lo siguiente:

Estado

Muestra el estado de la suscripción de un servidor de CA Enterprise Log Manager dado. Los estados de suscripción son Inactivo, En espera, Descargando, Instalando, Completado y Erróneo.

Mensaje

Muestra cualquier mensaje relacionado con el estado de suscripción de un servidor de CA Enterprise Log Manager dado.

Fecha

Muestra la fecha de la última acción de actualización de un servidor de CA Enterprise Log Manager dado.

Edición de la configuración de suscripción global

Durante la fase de implementación, se pueden configurar valores de configuración de suscripción globales para el entorno. Todos los servidores de CA Enterprise Log Manager heredan y utilizan esta configuración global, a menos que se anule la configuración global, lo cual se puede hacer si se configuran valores locales para un servidor individual.

De forma predeterminada, el primer servidor instalado es el proxy de suscripción predeterminado y todos los servidores instalados posteriormente se configuran como clientes de suscripción. Si no hay ningún otro proxy configurado o disponible, el proxy predeterminado descarga las actualizaciones en los clientes de suscripción.

Se puede cambiar la configuración global en cualquier momento. Todos los servidores heredan los cambios realizados, a menos que un servidor específico esté configurado localmente para ignorar esta configuración.

Los ajustes que se pueden realizar y editar en el ámbito global incluyen:

- Proxy de suscripción predeterminado
- Clave pública - Versión
- Proxys de suscripción para las actualizaciones de contenido

Para editar la configuración de suscripción global

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Haga clic en Servicio de suscripción.

Aparecerá la configuración de servicio global para el servicio de suscripción.

3. Haga clic en la ficha Administración.
4. En el panel derecho, examine los valores del servicio de suscripción de la configuración de servicio global. Revise la configuración y haga cualquier cambio que sea necesario.

Nota: Consulte la ayuda en línea para obtener información detallada sobre los campos.

5. Haga clic en Guardar.

Más información:

[Aplicación de actualizaciones de suscripción](#) (en la página 687)

Edición de la configuración de suscripción local de los servidores

Durante la implementación de suscripciones, se puede establecer una configuración global de suscripción para el entorno, como por ejemplo una programación de suscripción o una lista de proxys. Los servidores de CA Enterprise Log Manager individuales heredan esta configuración global.

Se puede anular en cualquier momento la configuración global si se configuran valores locales para servidores individuales. Se debe tener en cuenta el rol de suscripción de los servidores cuando se planifique anular la configuración global.

Para editar la configuración de suscripción de los servidores

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda Servicio de suscripción y seleccione el servidor que va a configurar.
Aparecerá la configuración del servicio de suscripción del servidor de CA Enterprise Log Manager seleccionado.
3. Haga clic en la ficha Administración.

4. Si desea cambiar el rol de suscripción de un servidor, realice una de las siguientes acciones:
 - Para designarlo como un cliente de suscripción, desactive la casilla de verificación ¿Proxy de suscripción?
 - Para designarlo como un proxy de suscripción en línea, seleccione la casilla de verificación ¿Proxy de suscripción? y seleccione Proxy de suscripción en línea.
 - Para designarlo como un proxy de suscripción sin conexión, seleccione la casilla de verificación ¿Proxy de suscripción? y seleccione Proxy de suscripción sin conexión.

Nota: Antes de cambiar el rol de un servidor de proxy de suscripción a cliente de suscripción, tenga en cuenta las configuraciones de los clientes de suscripción que utilizan este proxy. Si pasa un servidor de proxy a cliente, deberá eliminar de inmediato ese servidor de los proxys de suscripción globales y locales en las listas de actualizaciones para clientes.

Importante: Antes de cambiar el rol de un servidor y convertirlo en un proxy de suscripción sin conexión, deberá tener en cuenta si éste está incluido en alguna lista de proxys. En entornos de suscripción mixtos, donde se hayan configurado proxys de suscripción tanto en línea como sin conexión, no se deben incluir los proxys sin conexión en la lista de proxys de ninguno de los clientes de suscripción en línea.

5. Para anular una configuración global heredada, haga clic en el botón de alternancia entre los ámbitos global y local para cambiar a la configuración de servicio local para el campo seleccionado.

Nota: Para restaurar la configuración global, haga clic de nuevo en el botón. La configuración global se restaura a la hora de inicio de la siguiente actualización.

6. Si los módulos que desea descargar para este servidor son distintos a los heredados de acuerdo con la configuración global, haga el cambio a configuración local, haga clic en Examinar y seleccione los módulos deseados.

Nota: Asegúrese de que los módulos seleccionados para los proxys de suscripción incluyen por lo menos todos los módulos seleccionados en las listas de descarga de los clientes que reciben actualizaciones de dichos proxys.

7. Si este servidor va a descargar actualizaciones de suscripción a través de un servidor proxy HTTP distinto al heredado, cambie a la configuración local y configure el proxy HTTP deseado.

8. Si desea que este servidor descargue actualizaciones con una programación diferente de la heredada, cambie a la configuración local y edite la programación.
9. Si desea que este servidor pueda descargar actualizaciones de otro proxy de suscripción de CA Enterprise Log Manager, cambie a la configuración local y agregue los servidores proxy de CA Enterprise Log Manager deseados a la lista de servidores proxy de suscripción para las actualizaciones del cliente.

Este servidor se pondrá en contacto con los servidores proxy especificados para descargar actualizaciones de suscripción y creará una estructura de distintos niveles proxy.
10. Haga clic en Guardar.

Descarga y selección de módulos para la suscripción sin conexión

Los archivos de suscripción sin conexión están disponibles en el sitio FTP de suscripción sin conexión de CA, comprimidos en formato .zip. A medida que aparecen nuevos módulos, estos se ofrecen en el sitio FTP. Controle la lista de módulos disponibles periódicamente para asegurarse de que se han descargado las actualizaciones más recientes. También puede conocer la disponibilidad de nuevas versiones y Service Pack del gestor de registros consultando el sitio de soporte de CA (<http://ca.com/support>).

Antes de que se puedan seleccionar módulos para la descarga para proxys de suscripción sin conexión, se deberá descargar el paquete de archivos de actualización sin conexión del sitio FTP de CA y copiarlo manualmente a los proxys sin conexión. A continuación, se pueden seleccionar qué módulos se van a descargar e instalar. Por lo contrario, los clientes de suscripción sin conexión reciben de forma automática todas las actualizaciones que se instalan manualmente en su respectivo proxy sin conexión, independientemente de los módulos que se hayan seleccionado para el cliente a nivel local.

Para descargar y seleccionar módulos de suscripción sin conexión

1. En sistemas que dispongan de acceso FTP o a Internet, desplácese hasta el sitio FTP de suscripción sin conexión:

`ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription`

El índice del directorio muestra una carpeta para cada versión mayor de CA Enterprise Log Manager.

2. Descargue el archivo .zip adecuado, de acuerdo con la actualización que se vaya a efectuar.

Nota: La carpeta para la versión de CA Enterprise Log Manager r12.5 contiene una subcarpeta, además de un archivo .zip. La subcarpeta contiene módulos que permiten realizar la actualización de cualquier versión anterior a la versión r12.5. El archivo .zip contiene los módulos que permiten efectuar actualizaciones periódicas a la versión r12.5. Si está utilizando una suscripción sin conexión para realizar la actualización a la versión r12.5 desde una versión anterior, consulte el tema relativo a la actualización a CA Enterprise Log Manager en las *Notas de la versión*. Si está realizando una actualización rutinaria, seleccione el archivo .zip.

3. Copie manualmente el archivo .zip (a través de medios físicos como discos o scp), a la siguiente ruta de archivo en los proxys sin conexión:

`/opt/CA/LogManager/data/subscription/offline.`

4. Inicie sesión en un sistema dentro del entorno de CA Enterprise Log Manager.
5. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
6. Expanda Servicio de suscripción y seleccione el servidor proxy sin conexión que va a configurar.

Aparecerá la configuración del servicio de suscripción del servidor de CA Enterprise Log Manager seleccionado.

Nota: Los clientes de suscripción sin conexión reciben automáticamente todos los módulos que se instalan manualmente en su respectivo proxy sin conexión. El contenido del servidor proxy controla qué actualizaciones reciben los clientes de suscripción. Los módulos seleccionados en el nivel local para clientes sin conexión no tienen ningún efecto.

7. Haga clic en la ficha Administración.
8. En el cuadro desplegable Archivo, seleccione el archivo .zip que ha copiado en el servidor y haga clic en Examinar.
Aparecerá el cuadro de diálogo Módulos disponibles para descargar.
9. Seleccione los módulos que desee descargar.
10. Haga clic en Aceptar.
Se cerrará el cuadro de diálogo Módulos disponibles para descargar, y los módulos seleccionados aparecerán en la lista Módulos seleccionados para la descarga.
11. Haga clic en Guardar.
Llegados a este punto, los clientes de suscripción sin conexión pueden descargar estos módulos de forma automática, según la programación de suscripción determinada por el usuario, o a petición, al iniciar la actualización manual.
12. (Opcional) Haga clic en Actualizar ahora.
El servidor proxy sin conexión se actualizará con los módulos seleccionados.
Nota: Aunque se puede permitir que el proxy sin conexión se actualice siguiendo la programación de suscripción determinada por el usuario, es recomendable realizar una actualización manual siempre que se transfieran nuevos archivos. Esta práctica asegura que las actualizaciones se encontrarán disponibles cuando los clientes de suscripción sin conexión las soliciten.

Acerca de las actualizaciones a petición

Una actualización a petición es diferente de una actualización programada, ya que se realiza de inmediato y sólo actualiza el servidor seleccionado. Las actualizaciones a petición para un servidor de CA Enterprise Log Manager sólo se pueden invocar de una en una. Antes de realizar actualizaciones a petición en clientes de suscripción es necesario actualizar el servidor proxy.

Generalmente, las actualizaciones programadas mantienen actualizados todos los servidores de CA Enterprise Log Manager con los últimos archivos binarios y el servidor de gestión con la configuración y los archivos de contenido más recientes. Sin embargo, a veces es adecuado invocar una actualización no programada para un solo servidor.

En los casos siguientes, considere la posibilidad de usar actualizaciones a petición:

- Se informa de un error o una advertencia de evento de suscripción para el servidor de gestión, por ejemplo:

Failed to connect to EEMServer

Error installing content in EEM

Seleccione el servidor de gestión y haga clic en Actualizar ahora. Si el servidor de gestión se configura como el proxy para las actualizaciones de contenido, el servidor descarga nuevas actualizaciones del servidor de suscripción de CA. A continuación el servidor inserta las actualizaciones de contenido al repositorio de contenido. Si este servidor está configurado como un proxy para clientes, pone a disposición de sus clientes las actualizaciones binarias, en orden de llegada.

Nota: También se puede esperar hasta la siguiente sesión programada, momento en el cual se retoman y se completan los procesos que estuvieran incompletos.

- Un mensaje de error de evento de suscripción indica que se ha interrumpido la descarga. Si la descarga sólo se interrumpe en un servidor proxy, la realización de una actualización a petición intentará realizar la descarga de nuevo. Se recomienda utilizar una actualización a petición si se observa el error poco después de que se produzca. Si la hora de inicio entre el proxy y el cliente es suficiente, se podrá realizar una actualización a petición del proxy antes de comience la actualización programada por parte de los clientes que obtienen actualizaciones de ese proxy.
- Instala un nuevo CA Enterprise Log Manager, lo configura como un proxy y desea asegurarse de que se aplican las últimas actualizaciones antes de usarlo.
- Observa que un módulo necesario para un cliente no se ha seleccionado para descargarlo. Sin embargo, el proxy ha seleccionado ese módulo para la descarga. La ejecución de Actualizar ahora en los clientes instala las actualizaciones que faltan.
- Ha descargado un paquete de suscripción sin conexión y lo ha copiado en un proxy de suscripción sin conexión. Se puede realizar una actualización manual siempre que se transfieran nuevos archivos. Esto contribuye a asegurar que las actualizaciones estén disponibles siempre que los clientes de suscripción sin conexión las soliciten.

Inicio de actualizaciones a petición

Con la función Actualizar ahora, se pueden actualizar los servidores a petición. Cuando actualice dos o más servidores seguidos, compruebe que el proceso termina en uno de ellos antes de comenzar en el siguiente. Revise los eventos autocontrolados para obtener la confirmación.

En caso de haber modificado recientemente alguna configuración de suscripción, asegúrese de esperar a que transcurra el intervalo de actualización (de forma predeterminada, 300 segundos) antes de ejecutar una actualización a petición. CA Enterprise Log Manager generará un evento autocontrolado cuando finalice la actualización.

Nota: Si hay una actualización programada en curso, hacer clic en Actualizar ahora no tendrá ningún efecto. Si la hora de inicio de una actualización programada se produce mientras el proceso de actualización está en curso, no se ejecutará el proceso programado. Cuando finalice el proceso a petición se reanudarán los ciclos de actualización programados.

Importante: Si los módulos que se van a descargar contienen actualizaciones de contenido, será necesario actualizar el proxy de contenido antes de realizar cualquier otra actualización a petición.

Para actualizar servidores a petición

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda el servicio de suscripción en la lista de servicios.
3. Seleccione el servidor que funciona como proxy para actualizaciones de contenido y examine los módulos que se han seleccionado para la descarga. Si estos incluyen actualizaciones de contenido, haga clic en Actualizar ahora.

El servidor recupera las actualizaciones del servidor de suscripción de CA. Como proxy para actualizaciones de contenido, el servidor inserta actualizaciones de contenido al repositorio de contenido. Como proxy en línea, el servidor también descarga actualizaciones binarias.

4. Seleccione el servidor que vaya a actualizar y examine su función.
5. Si se trata de un proxy de suscripción para actualizaciones de clientes, haga clic en Actualizar ahora.

El servidor se actualizará con las actualizaciones binarias de los módulos seleccionados para la descarga.

6. Si se trata de un cliente con un proxy en línea, realice las siguientes acciones:

- a. Identifique un proxy para este cliente a partir de los elementos seleccionados en la lista de servidores proxy de suscripción para clientes.
- b. Seleccione el proxy para el cliente y haga clic en Actualizar ahora.
- c. Seleccione el cliente y haga clic en Actualizar ahora.

El servidor se actualizará con las actualizaciones binarias de los módulos seleccionados para la descarga.

7. Si se trata de un proxy de suscripción sin conexión, realice las siguientes acciones:

- a. Descargue el paquete de actualización sin conexión del sitio FTP de suscripción sin conexión de CA.
- b. Copie manualmente las actualizaciones en la ruta de descarga del proxy sin conexión:
.../data/subscription/offline
- c. Seleccione el proxy sin conexión y el archivo .zip de actualización sin conexión. A continuación, haga clic en Examinar y seleccione los módulos deseados.
- d. Haga clic en Actualizar ahora.

El servidor se actualizará con las actualizaciones binarias de los módulos seleccionados para la descarga.

8. Si se trata de un cliente con un proxy sin conexión, realice las siguientes acciones:

- a. Actualice el proxy sin conexión como se describió en el paso 7.
- b. Seleccione el cliente y haga clic en Actualizar ahora.

El servidor se actualizará con todos los módulos instalados en su proxy sin conexión.

Nota: Los clientes de suscripción sin conexión reciben automáticamente todos los módulos que se instalan manualmente en su respectivo proxy sin conexión. Los módulos seleccionados en el nivel local para clientes sin conexión no tienen ningún efecto.

Espacio libre en disco para actualizaciones

Para asegurarse de que las actualizaciones de suscripciones se realizan correctamente en los servidores de CA Enterprise Log Manager, limpie el disco regularmente. Nota: Si el espacio en disco disponible es inferior a 5 GB cuando comience el proceso de actualización de la suscripción, el servicio de suscripción emitirá un evento autocontrolado y suspenderá el proceso de descarga.

Para garantizar que existe suficiente espacio en el disco para las actualizaciones de suscripción

1. Controle el espacio libre en el disco de forma regular. Como alternativa, es posible configurar una alerta de acción para recibir un aviso cuando el espacio libre en disco esté por debajo de la cantidad especificada.
2. Libere espacio en el disco mediante una herramienta de limpieza del disco.
3. Si se le advierte de la necesidad de realizar una limpieza mediante un evento autocontrolado, libere suficiente espacio en el disco como para permitir que la descarga continúe.

Más información:

[Ejemplo: Crear una alerta de acción para el espacio en disco bajo](#) (en la página 486)

Acerca de las claves públicas de suscripción

El proxy de suscripción mantiene un conjunto de claves públicas correspondientes a las claves privadas empleadas por el servidor de suscripciones de CA. El proxy de suscripción descarga actualizaciones de suscripción como un archivo comprimido que se firma de forma digital mediante una clave privada. La actualización identifica la clave pública que se debe emplear para comprobar la firma de la actualización. La verificación de la firma es el método que emplea el proxy de suscripción para asegurarse de que la actualización procede del servidor de actualizaciones de CA. Sólo existe un par de claves pública-privada empleado para una operación de suscripción determinada. Se emplea una clave privada para firmar la actualización; se emplea una clave pública para verificar la firma. La clave pública se guarda en cada servidor de CA Enterprise Log Manager y se puede actualizar.

CA Enterprise Log Manager almacena la versión inicial de la clave pública en el archivo de configuración de suscripción durante la instalación. Si es necesaria una clave privada nueva, la clave pública asociada se descarga con la actualización de suscripción antes del ciclo de actualización en el lugar donde se necesita la nueva clave.

Importante: No actualice de forma manual el campo Clave pública para la suscripción si no obtiene instrucciones específicas del Soporte técnico de CA.

Eventos autocontrolados para suscripción

Puede controlar los estados correctos o incorrectos de los procesos de actualización de suscripción que afectan a servidores de CA Enterprise Log Manager configurados del modo siguiente:

- Proxy de suscripción predeterminado
- Otros proxys de suscripción en línea si los hay
- Proxys de suscripción sin conexión si los hay
- Clientes de suscripción

Nota: Los eventos descritos aquí no realizan el seguimiento de actualizaciones de suscripción para agentes.

Se indican los procesos correctos de las siguientes acciones:

- Arranque y apagado de los servidores de CA Enterprise Log Manager, tanto proxys de suscripción como clientes de suscripción.
- Descarga correcta del componente de un proxy de suscripción en línea o sin conexión en un cliente de suscripción
- Instalación correcta de un componente por parte de un cliente de suscripción

Se indican los fallos y los errores siguientes:

- Descarga incorrecta del componente de un proxy de suscripción en línea o sin conexión en un cliente de suscripción
- Error al instalar un componente por parte de un cliente de suscripción
- Condiciones de error

Control de los eventos de suscripción

Puede controlar si los procesos de actualización de suscripción son correctos o no mediante la visualización de los eventos autocontrolados de la suscripción.

Para controlar los eventos de procesamiento de suscripción

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Haga clic en el servicio de suscripción en la lista de servicios.
3. Haga clic en la ficha Eventos autocontrolados tanto para el servicio de suscripción como para un host que aparezca en la lista Servicio de suscripción.

4. Revise los detalles del evento que se muestra.

Algunos de los campos mostrados en los eventos autocontrolados reflejan el método estándar de la gramática de eventos comunes para referirse a acciones comunes entre los proveedores. El modelo ideal se basa en esta jerarquía: `event_category`, `event_class` (dentro de la categoría), `event_action` (dentro de la clase), `event_result` y `event_severity`. La severidad de CA mostrada en este informe es la interpretación de CA de la severidad.

Severidad de CA

Gravedad del evento, donde

- Desconocido: eventos desconocidos, eventos no asignados a la gramática de eventos comunes o eventos sin clasificar
- Información: información sobre operaciones generales del sistema, información relacionada con la seguridad o un aviso
- Advertencia: cambios poco corrientes, una condición normal pero significativa, operaciones erróneas o rendimiento reducido
- Impacto menor: impacto menor en un sistema, una función o la seguridad
- Impacto mayor: impacto mayor en un sistema, una función o la seguridad
- Crítico: es necesaria una acción inmediata; es probable que haya una infracción de seguridad

Fecha

Fecha en la que se originó el evento.

Destinatario

Componente que no pudo finalizar correctamente el proceso actual. Podría tratarse de un proxy de suscripción o de un cliente de suscripción. Si se trata de un proxy de suscripción, puede ser un proxy predeterminado, un proxy en línea o un proxy sin conexión.

Host de receptor

Nombre del host del servidor de CA Enterprise Log Manager que es el receptor.

Categoría

Categoría del evento. La gestión de configuraciones es el campo `event_category` de los eventos de servicio de suscripción.

Usuario

El nombre de usuario o identidad que inició la acción que se expresa en la información del evento. Este es el campo `source_username` en la gramática de eventos comunes.

Acción

Acción que ha provocado la generación del evento. Este es el campo `event_action` en la gramática de eventos comunes.

Resultado

C de Correctamente; E de Error. El resultado de la acción de evento es el campo `event_result` en la gramática de eventos comunes. Otras acciones son Aceptar, Rechazar, Anular y Desconocido.

Descripción del resultado

Texto del mensaje. Si la columna de resultado muestra Error, lea el texto de Descripción del resultado.

5. Visualice los detalles en el visor de eventos. Aquí, puede ver cambios como los que se realizan en un valor de configuración como la hora de inicio de la actualización.

```
El cambio de configuración para el atributo (UpdateStartTime) Nuevo valor::[17] Se ha actualizado con éxito a archivo local en calmsunbulldtest01 para la suscripción
event_category=Configuration Management,event_class=Configuration Management,event_action=Configuration Change,event_sequence=Configuration Change,ideal_model=Security Management
System,event_count=1,event_logname=CALM,event_summarized=F,receiver_name=Subscription,receiver_version=12.0.0.19,receiver_hostname=calmsunbulldtest01,receiver_hostaddress=130.200.137.21
1,receiver_hostdomainname=ca.com,receiver_timezone=-
14400,receiver_time_gmt=1202765008,receiver_processid=3922,receiver_processname=igateway,dest_objectclass=Subscription,dest_objectname=Subscription,event_source_hostname=calmsunbulldtest
01,event_result=S,result_string= Configuration change for Attribute (UpdateStartTime) New value : [17] has been updated successfully to local file on calmsunbulldtest01 for Subscription
```

Visualización de detalles de eventos de suscripción

Después de configurar la suscripción, puede visualizar los eventos autocontrolados. Tras la actualización de una suscripción, puede verificar si la actualización de cada servidor se ha realizado correctamente. A medida que finalizan las actualizaciones, busque los mensajes de eventos autocontrolados siguientes en cada servidor afectado:

- <componente> se ha descargado correctamente en el proxy <nombreproxy> y se ha instalado en EEM.
- <componente> se ha descargado correctamente en el proxy <nombreproxy>.
- <componente> se ha instalado correctamente en el cliente <nombrecliente>.

También puede visualizar eventos autocontrolados de suscripción destinados a la solución de problemas.

Para visualizar los detalles de eventos de suscripción en el visor de eventos

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Haga clic en el servicio de suscripción en la lista de servicios.
3. Haga clic en la ficha Eventos autocontrolados tanto para el servicio de suscripción como para un host que aparezca en la lista Servicio de suscripción.
4. Examine la columna Descripción del resultado. Por ejemplo, esta columna puede mostrar eventos como "El cliente de suscripción no tiene módulos seleccionados para obtener actualizaciones".

Descripción de los resultados	
Subscription Client - calmrhbuildtest01 is communicating with the proxy - calmrhbuildtest01 for getting the Subscription updates.	
Subscription client has no modules selected for getting updates. Please select the modules for getting the updates from the Proxy.	
Unable to connect to the specified RSSFeed URL. Please check the URL again.	
Unable to connect to the specified RSSFeed URL. Please check the URL again.	
No modules are selected for getting updates. Please select the modules for getting the updates from the Subscription server.	

5. Haga doble clic en la descripción del resultado cuyos detalles desee revisar. Se abre el visor de eventos.
6. Desplácese hacia abajo a la sección de resultados y revise el texto que corresponde a result_string.

Visor de eventos - Detalles del evento - Detalles de los eventos autocontrolados del sistema		
Copiar ☒ Ocultar filas vacías		
Mostrar	Nombre	Valor
☒	event_result	S
☐	result_string	Get Integration Config successful. objectName [CA_Federation_Manager] Type [xmp] Object ID [ICALM_Configuration/Content/Parsing/CA_Federation_Manager_12.0.5009.0.XMPS]

Aplicación de actualizaciones de suscripción a agentes y conectores

Las actualizaciones periódicas, los service packs y las versiones puntuales se entregan con la suscripción. A menudo, los módulos que se descargan incluyen agentes e integraciones. Cuando estos módulos se descargan en un cliente de suscripción que gestiona agentes, debe aplicar estas actualizaciones en los agentes tras verificar que el cliente de suscripción que gestiona los agentes se haya actualizado de forma correcta. Las actualizaciones en los agentes deben aplicarse antes que las actualizaciones en los conectores.

Para actualizar agentes de CA Enterprise Log Manager con actualizaciones de suscripción

1. Si la actualización incluye el módulo de agentes, actualice los agentes por plataforma del modo siguiente:
 - a. Haga clic en la ficha Administración y en la subficha Recopilación de registros.
 - b. Determine si desea aplicar las actualizaciones de agentes a todos los agentes a la vez, a un grupo de agentes seleccionados o a un agente en particular, en función del nivel en el que se aplique una plataforma en concreto.
 - Si todos los agentes se instalan en la misma plataforma, seleccione Explorador de agentes y, a continuación, haga clic en Suscripción.
 - Si los grupos de agentes están formados por agentes instalados en la misma plataforma, expanda Explorador de agentes, seleccione un grupo de agentes y, a continuación, haga clic en Suscripción.
 - Si no es así, expanda Explorador de agentes, expanda un grupo de agentes, seleccione un agente y, a continuación, haga clic en Suscripción.

Aparece el asistente de suscripción.

 - c. Si ha seleccionado Explorador de agentes o un grupo de agentes, seleccione Actualizaciones del agente, seleccione la plataforma en la lista desplegable Plataforma, haga clic en Buscar y haga clic en el paso de selección de la versión.
 - d. Si ha seleccionado un agente, seleccione Actualizaciones del agente y haga clic en el paso de selección de la versión.
 - e. Seleccione la versión de la actualización de cada agente de la lista.
 - f. Haga clic en Guardar y cerrar.

- g. Compruebe que todo es correcto. Haga clic en Estado y comando. Haga clic en la opción de configuración correcta. Anote la versión de la configuración que se ha aplicado.
 - h. Repita esta acción las veces que sean necesarias para actualizar todos los agentes.
 2. Si la actualización incluye el módulo de integraciones, actualice los conectores de los agentes del modo siguiente:
 - a. Haga clic en la ficha Administración y en la subficha Recopilación de registros.
 - b. Determine si desea aplicar actualizaciones de conectores a todos los conectores de todos los agentes a la vez, a los conectores de los agentes de un grupo de agentes seleccionado o a los conectores de un agente en particular.
 - c. Seleccione Explorador de agentes, un grupo de agentes o un agente. A continuación, haga clic en Suscripción.
 - d. Seleccione Actualizaciones del conector en la lista de selección de actualizaciones.
 - e. También puede seleccionar un valor de una o varias de las listas desplegables siguientes para modificar la configuración predeterminada, Todos: Grupo de agentes, Plataforma, Integración. Haga clic en Buscar.
 - f. Haga clic en el paso de selección de versiones.
 - g. Haga clic en Seleccionar todo para seleccionar todos los miembros de la lista o seleccione una a una las filas que correspondan al conector que desea actualizar. Para cada fila seleccionada, elija la versión de la actualización que va a aplicar.
 - h. Haga clic en Guardar y cerrar.
3. Verifique las actualizaciones. Vuelva a ejecutar el asistente de suscripción. Seleccione el paso de selección de versiones para visualizar la versión actual y verificar que se trata de la versión seleccionada para realizar la actualización. Haga clic en Cancelar.

Más información:

[Aplicación de actualizaciones de suscripción](#) (en la página 687)

[Apertura del asistente de listas de actualizaciones](#) (en la página 688)

[Selección de los agentes o conectores que se van a actualizar](#) (en la página 689)

[Actualización de versiones de integración de agentes o conectores](#) (en la página 690)

Capítulo 8: Filtros y perfiles

Esta sección contiene los siguientes temas:

- [Filtros globales y locales](#) (en la página 261)
- [Creación de perfiles](#) (en la página 265)
- [Importación de perfiles](#) (en la página 269)
- [Exportación de perfiles](#) (en la página 270)
- [Establecimiento de perfiles](#) (en la página 270)
- [Creación de filtros globales](#) (en la página 271)
- [Configuración de los ajustes de consultas globales](#) (en la página 273)
- [Edición de filtros globales](#) (en la página 274)
- [Eliminación de filtros globales](#) (en la página 274)
- [Creación de filtros locales](#) (en la página 275)
- [Edición de filtros locales](#) (en la página 276)
- [Eliminación de filtros locales](#) (en la página 276)

Capítulo 9: Filtros globales y locales

Puede establecer o editar filtros para refinar el evento mostrado o la información del incidente. Puede acceder al cuadro de diálogo de filtro global de la ventana principal de CA Enterprise Log Manager. Puede agregar filtros locales desde una visualización de informe o consulta individual, o desde el área Incidentes. También puede emplear la interfaz de filtro global para establecer la configuración de consultas en toda la aplicación.

Cada tipo de filtro cuenta con un cuadro de diálogo de creación propio que se inicia mediante un único botón:

Filtro global

Se aplica a todos los informes o consultas que se visualizan sólo en la sesión *en curso* y proporciona una forma de visualizar una gran variedad de tipos de eventos categorizados de forma idéntica. Aparecerá el botón Filtro global en la parte superior de la ventana principal de CA Enterprise Log Manager encima del menú Servidor del gestor de registros. Puede usar un filtro global para visualizar todos los eventos recibidos la semana pasada, o de un host determinado, por ejemplo. Puede establecer también filtros globales para Incidentes, que se elaboran de la misma manera, pero se aplican solamente a los incidentes y a la información del evento de los componentes que le corresponden.

Nota: El ajuste predeterminado es el de un filtro global que devuelve las últimas 6 horas de datos.

Filtro local

Se aplica solamente a la vista de informe, consulta o incidente en curso. El botón Filtro local aparece en la parte superior del panel de detalles en las visualizaciones de consultas o informes, y en la parte superior del panel Incidentes. Cuando visualiza un nuevo informe, el filtro local no se aplica o guarda, a menos que guarde el informe como favorito con ese filtro configurado. Los filtros locales le permiten reducir una vista actual para ver sólo un host en una vista de informe de varios host, por ejemplo, sin cambiar otras vistas de informe.

Esta sección contiene los siguientes temas:

[Acerca de los filtros simples](#) (en la página 262)

[Establecimiento de filtros simples](#) (en la página 263)

[Acerca de los filtros de perfiles](#) (en la página 264)

Acerca de los filtros simples

Antes de utilizar por primera vez el asistente de diseño de consulta o el asistente de diseño de perfil, familiarícese con los tipos de filtros simples.

Ejemplos de filtros simples

A continuación, se muestra un ejemplo de cada tipo de filtro simple:

Tipo de filtro	Valor	Descripción
Modelo ideal	Antivirus	Sólo muestra datos de eventos generados por productos como los siguientes: ■ CA Anti-Virus ■ McAfee VirusScan ■ Symantec Antivirus Corporate Edition ■ TrendMicro OfficeScan
Categoría de evento/ Clase de evento	Actividad de acceso al sistema/inicio de sesión	Sólo muestra datos de eventos relacionados con usuarios que inician sesión en un sistema.
Nombre de registro de eventos	Cisco PIX Firewall	Sólo muestra los datos de eventos que generan los dispositivos de Cisco PIX Firewall.

Exceptuando el nombre de registro de eventos, los tipos de filtros se basan en la gramática de eventos comunes (CEG).

- Para obtener información acerca de los filtros basados en tecnologías/productos, consulte la lista de modelos ideales.
- Para obtener información acerca de los filtros basados en categorías/clases/acciones, consulte la lista de categorías de eventos y la lista de clases de eventos.

Busque esas listas en la ayuda en línea, en la sección de la gramática de eventos comunes.

Establecimiento de filtros simples

Puede definir filtros simples para establecer criterios para los datos de eventos que desea visualizar o cuyos informes desea generar. Al definirlos en el asistente de diseño de consulta, los filtros simples le permiten limitar los datos de eventos obtenidos tras una consulta empleada en un informe o una alerta. Al definirlos en el asistente de diseño de perfil, los filtros simples limitan los datos visualizados en los resultados de informes o de consultas cuando se aplica el perfil.

1. Abra el asistente.
2. Determine el tipo de filtro simple que desea definir:
 - basado en tecnologías.
 - basado en categorías, basado en categorías y clases o basado en categorías, clases y acciones.
 - basado en productos.
3. Para establecer un filtro basado en tecnologías, haga clic en la casilla de verificación *El modelo ideal es y*, a continuación, seleccione un valor en la lista desplegable del modelo ideal.
4. Para definir un filtro basado en la categoría, la categoría y la clase, o la categoría, la clase y la acción de un evento de seguridad, lleve a cabo las acciones siguientes:
 - a. Haga clic en la casilla de verificación *Categoría de evento y*, a continuación, seleccione un valor en la lista desplegable asociada.
 - b. (Opcional). Haga clic en la casilla de verificación *Clase de evento y*, a continuación, seleccione un valor en la lista desplegable.
 - c. (Opcional). Si ha seleccionado *Clase de evento*, haga clic en la casilla de verificación *La acción del evento es y*, a continuación, seleccione un valor en la lista desplegable.

Nota: También puede definir este filtro de tipo en un filtro basado en tecnologías.

5. Para establecer un filtro basado en productos, haga clic en la casilla de verificación *El nombre del registro de eventos es y*, a continuación, seleccione un valor en la lista desplegable.
6. Siga los pasos que le indique el asistente.

Acerca de los filtros de perfiles

Un perfil es un conjunto de filtros. Puede crear un perfil mediante filtros de etiquetas, filtros de datos o una combinación. El filtro de etiquetas de consulta limita las consultas mostradas para su selección; el filtro de etiquetas de informe limita los informes mostrados para su selección. Los filtros de datos limitan los datos que se muestran en los resultados de una consulta o un informe. Los filtros de perfiles se aplican a consultas, informes, alertas programadas e informes programados.

Puede seleccionar filtros de etiqueta para informes y consultas por separado. Los filtros de etiquetas incluyen, entre otros, los siguientes:

- Etiquetas basadas en estándares, como COBIT, FISMA, GLBA, HIPAA, NERC, PCI, SAS 70, SOX.
Los filtros de etiquetas basadas en estándares se aplican a etiquetas de informes, no a etiquetas de consultas.
- Etiquetas de categorías de eventos de seguridad, como la seguridad del contenido, la seguridad de host, la seguridad de red, la seguridad operativa, el acceso a los recursos o el acceso al sistema.
- Etiquetas de productos, como CA Access Control, CA Identity Manager y CA SiteMinder.

Puede seleccionar un filtro de datos simple o puede crear un filtro de datos avanzado. A continuación, se muestra una breve descripción de cada uno:

- Los filtros de datos simples pueden basarse en uno de los elementos siguientes:
 - Una tecnología seleccionada (software del sistema, servicios y software de la aplicación de host, servicios y software de la aplicación de red)
 - Una categoría de eventos seleccionada de la gramática de eventos comunes, una clase y una categoría de eventos seleccionadas de la gramática de eventos comunes, o una acción, una clase y una categoría de eventos seleccionadas de la gramática de eventos comunes
 - Un producto seleccionado
- Los filtros de datos avanzados se basan en una consulta de SQL definida por el usuario y formada por una o varias cláusulas WHERE. La consulta selecciona una columna de la gramática de eventos comunes con la cláusula WHERE formada por dicha columna, un operador seleccionado y un valor especificado.

Creación de perfiles

Puede crear perfiles que permitan a los usuarios restringir las vistas de CA Enterprise Log Manager en función de las necesidades del entorno. Por ejemplo, puede crear un perfil de CA Access Control que sólo muestre informes, consultas y eventos relevantes para Access Control.

El proceso de creación de un perfil mediante el asistente de perfiles consta de los pasos siguientes:

1. Apertura del asistente de perfiles
2. Asignación de un nombre al perfil e introducción de información de descripción
3. Identificación de la información mostrada mediante filtros simples y avanzados
4. Selección de las consultas e informes que se visualizan mediante filtros de etiquetas

Más información:

[Adición de detalles de perfiles](#) (en la página 266)

[Creación de filtros de datos](#) (en la página 267)

[Creación de filtros de etiquetas](#) (en la página 268)

Apertura del asistente de perfiles

Para crear un perfil nuevo o editar uno existente, debe abrir el asistente de perfiles.

Para abrir el asistente de perfiles

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.

Aparecerá la lista de carpetas Biblioteca.

2. Seleccione la carpeta Perfiles.

Los botones de perfiles aparecen en el panel de detalles.

3. Haga clic en Nuevo perfil. 

Se abre el asistente de perfiles.

Al emplear el asistente:

- Haga clic en Guardar para guardar el archivo de la regla sin cerrar el asistente.
- Haga clic en Guardar y Cerrar para guardar el archivo de la regla y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Adición de detalles de perfiles

Debe nombrar un perfil. También puede introducir información descriptiva opcional como referencia.

Para nombrar un perfil

1. Abra el asistente de perfiles.
2. Introduzca un nombre para el perfil nuevo. El nombre puede tener un máximo de 80 caracteres y puede incluir caracteres especiales.
3. (Opcional) Introduzca información descriptiva.
4. Vaya al paso de filtros de datos.

Creación de filtros de datos

Puede filtrar la información mostrada por el perfil mediante filtros simples o avanzados. Cada perfil debe tener al menos un filtro.

Para establecer filtros de datos de perfiles

1. Abra el asistente de perfiles.
2. Introduzca el nombre del perfil, si no se ha especificado aún, y vaya al paso Filtros de datos.

Aparece el cuadro de diálogo de filtros, donde se muestra la ficha Filtros simples.

3. Cree los filtros simples que desee. Por ejemplo, puede seleccionar la casilla de verificación Nombre de registro de eventos e introducir "CA Access Control" para buscar eventos de CA Access Control.
4. (Opcional) Haga clic en la ficha Filtros avanzados.

Aparece el cuadro de diálogo de filtros avanzados.

5. Agregue filtros avanzados según sea necesario.
6. Haga clic en la flecha correspondiente para avanzar al paso del asistente de perfiles que quiera completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el perfil nuevo aparece en la lista; si no es así, aparece el paso del asistente que haya seleccionado.

Más información

[Creación de un filtro de evento simple](#) (en la página 594)

[Creación de filtros de eventos avanzados](#) (en la página 597)

[Uso de filtros avanzados](#) (en la página 509)

Creación de filtros de etiquetas

Puede crear filtros de etiquetas para el perfil, controlando las etiquetas de categorías de consultas o informes que aparecen en la interfaz de CA Enterprise Log Manager cuando un usuario aplica el perfil. Por ejemplo, si crea un filtro de etiquetas para CA SiteMinder, la interfaz de CA Enterprise Log Manager sólo mostrará los informes y las consultas que contengan la etiqueta CA SiteMinder.

Para crear filtros de etiquetas

1. Abra el asistente de perfiles.
2. Introduzca el nombre del perfil, si no se ha especificado aún, y vaya al paso de filtros de etiqueta.

Aparece el cuadro de diálogo de filtros, que muestra la subficha Filtros de etiqueta de informe.
3. Haga clic en Nuevo filtro de evento.

Se activa la primera fila de la tabla de filtros de etiquetas.
4. Haga clic en la celda Etiqueta y seleccione o escriba el nombre de la etiqueta de la consulta o el informe que desee mostrar. Si lo escribe, la pantalla restringirá los nombres de etiquetas disponibles a medida que escribe.
5. (Opcional) Haga clic en Nuevo filtro de evento otra vez para agregar más filtros.

La segunda fila de la tabla de filtros se activa y muestra AND en la columna lógica.
6. (Opcional) Haga clic en la celda lógica para seleccionar un operador AND u OR.
7. (Opcional) Haga clic en la celda Etiqueta o escriba el nombre de la etiqueta que desee mostrar. Si lo escribe, la pantalla restringirá los nombres de etiquetas disponibles a medida que escribe.
8. (Opcional) Haga clic en las celdas de paréntesis de apertura y cierre e introduzca el número de paréntesis que necesita.
9. (Opcional) Haga clic en la subficha Filtros de etiqueta de consulta y repita los pasos del 3 al 8 para crear los filtros de etiquetas de consultas que necesite.
10. Haga clic en Guardar cuando haya introducido todas las instrucciones de filtro que quiera.

Más información:

[Creación de filtros de datos](#) (en la página 267)

Importación de perfiles

Puede importar perfiles pudiendo desplazar perfiles de un entorno a otro. Por ejemplo, puede importar un perfil creado en un entorno de prueba al entorno real.

Para importar perfiles

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.
Aparecerá la lista de carpetas Biblioteca.
2. Haga clic en la flecha junto a la carpeta Perfiles para expandirla.
Los botones de perfiles aparecen en el panel de detalles.
3. Haga clic en Importar perfil.
Aparece el cuadro de diálogo de importación de archivo.
4. Busque el archivo que desea importar y haga clic en Aceptar.
Aparece el asistente de perfiles y muestra los detalles del perfil seleccionado.
5. Realice los cambios deseados y haga clic en Guardar y cerrar. Si el perfil importado tiene el mismo nombre que otro perfil que ya se encuentra en la base de datos de gestión, deberá cambiarle el nombre.
El perfil importado aparece en la carpeta correspondiente.

Exportación de perfiles

Es posible exportar perfiles. Esto le permite compartir perfiles en distintos entornos. Por ejemplo, puede exportar un perfil creado en un entorno de prueba al entorno real.

Para exportar perfiles

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.
Aparecerá la lista de carpetas Biblioteca.
2. Haga clic en la flecha junto a la carpeta Perfiles para expandirla.
Aparecerán las carpetas de los perfiles.
3. Haga clic en la carpeta que contiene el perfil que desea exportar.
La carpeta se expande y muestra los archivos.
4. Seleccione el perfil que desea exportar y, a continuación, haga clic en Exportar perfil.
Aparece un cuadro de diálogo de ubicación de exportación.
5. Introduzca o busque la ubicación en la que desea almacenar el perfil exportado y haga clic en Guardar.
Aparece un cuadro de diálogo de confirmación de exportación correcta.
6. Haga clic en OK.
El perfil se exporta.

Establecimiento de perfiles

Puede seleccionar cualquier perfil disponible para aplicarlo al entorno, restringiendo las consultas y los informes disponibles en función de las condiciones del perfil. Para establecer un perfil, seleccione el perfil deseado en el menú desplegable Perfiles situado en la parte superior de la ventana principal de CA Enterprise Log Manager.

Nota: Para establecer el perfil seleccionado como el perfil predeterminado del entorno, haga clic en la opción Establecer como perfil predeterminado en la parte superior de la ventana principal de CA Enterprise Log Manager. El perfil seleccionado se establecerá como el perfil predeterminado para el usuario conectado.

Creación de filtros globales

Puede crear filtros globales. Los filtros globales le permiten ver todos los informes, consultas e incidentes mediante los mismos factores de calificación. Cuando crea un filtro global, elige si se aplica a eventos o a incidentes. Un solo filtro global no se puede aplicar a los dos. También puede emplear la interfaz de filtro global para establecer la configuración de consultas en toda la aplicación.

Para crear filtros globales

1. Haga clic en el botón Filtros globales que aparece en la parte superior de la ventana principal.
Aparecerá el cuadro de diálogo Filtros y valores de configuración globales.
2. Haga clic en la ficha Eventos o en la ficha Incidentes para seleccionar el ámbito de aplicación del filtro global.
3. Especifique el período de tiempo que desea definir como filtro de búsqueda mediante la lista desplegable Intervalo de tiempo.
4. Seleccione la casilla de verificación Coincidencia para introducir un valor específico mediante el cual filtrar todos los eventos sin formato disponibles.

Nota: Puede buscar varios valores, frases o valores parciales en los eventos sin formato mediante la sintaxis especializada de coincidencia.

5. Haga clic en Agregar filtro para especificar los campos de evento que quiere incluir en el filtro.

Aparece el menú desplegable Columna y un campo de entrada Valor.

6. Elija el campo de eventos que quiera incluir en el filtro e introduzca el valor que debe tener el campo para que se muestre en los informes filtrados. Puede introducir varios valores y nombres de campos de eventos haciendo clic nuevamente en Agregar filtro. Si selecciona el botón Excluir, se incluyen todos los valores *excepto* el que introdujo para el nombre de campo del evento elegido.

Nota: Si crea un filtro global en un campo de tipo cadena, se agregará a la lista de filtros rápidos. Si crea un filtro en un campo numérico o de hora, se agregará a la lista de filtros avanzados.

7. (Opcional) Haga clic en la ficha Filtros avanzados para agregar más calificadores.
8. (Opcional) Haga clic en la ficha Configuración para seleccionar la configuración global. Esta configuración se utilizará en toda la aplicación.

9. (Opcional) Seleccione la opción Establecer como predeterminado en la parte inferior del cuadro de diálogo para retener la configuración de filtro para sesiones futuras, siempre y cuando inicie sesión como el mismo usuario.

10. Haga clic en Guardar.

El cuadro de diálogo Filtros y valores de configuración globales se cierra y el nuevo filtro se aplica a los informes.

Más información:

[Uso de filtros avanzados](#) (en la página 509)

[Configuración de los ajustes de consultas globales](#) (en la página 273)

Configuración de los ajustes de consultas globales

Mediante el cuadro de diálogo de filtros globales, puede establecer condiciones que afecten a toda la aplicación y que se apliquen a todos los informes y consultas del entorno. La configuración global se aplica en toda la sesión actual, a no ser que la establezca como predeterminada.

Para configurar los ajustes de consultas globales

1. Haga clic en el botón Filtros globales que aparece en la parte superior de la ventana principal.

Aparece el cuadro de diálogo Filtros y valores de configuración globales, que incluye la ficha Filtros rápidos.

2. Haga clic en la ficha Configuración.

La ficha se abre y muestra los valores siguientes.

Zona horaria local

Controla la zona horaria de todos los campos de fecha/hora de los informes y las consultas. Los informes y las consultas adoptan la zona horaria seleccionada en la lista desplegable en lugar de emplear la zona horaria del servidor de CA Enterprise Log Manager.

Ejecutar consultas sobre datos federados

Permite aplicar la consulta en todos los servidores federados disponibles. Este ajuste está activado de forma predeterminada. La desactivación de este ajuste hace que las consultas sólo se apliquen a los datos de eventos almacenados en el sistema de almacenamiento de registro de eventos. Esto le permite comprobar rápidamente el sistema de almacenamiento de registro de eventos cuando sabe que los eventos de destino son locales.

Activar actualización automática de consultas

Permite que la pantalla se actualice automáticamente tras los intervalos definidos para cada consulta.

3. (Opcional) Seleccione Establecer como predeterminado en la parte inferior del cuadro de diálogo para mantener la configuración como valores predeterminados que se retendrán tras la sesión actual.

4. Realice los cambios deseados y haga clic en Guardar.

El cuadro de diálogo Filtros y valores de configuración globales se cierra y aparece el filtro nuevo.

Edición de filtros globales

Puede editar los filtros globales existentes.

Para editar filtros globales

1. Haga clic en el botón Filtros globales que aparece en la parte superior de la ventana principal.

Aparece el cuadro de diálogo Filtros y valores de configuración globales, que incluye la ficha Filtros rápidos.

2. Cambie o agregue parámetros según sea necesario. Puede eliminar el parámetro de un filtro rápido aislado haciendo clic en el icono Suprimir que se encuentra a su lado.
3. Haga clic en Guardar.

El cuadro de diálogo Filtros y valores de configuración globales se cierra y se aplica el filtro editado.

Eliminación de filtros globales

Puede eliminar filtros globales y hacer que todos los informes vuelvan al estado predeterminado.

Para eliminar un filtro global, haga clic en el botón para borrar filtros globales situado en la parte superior de la ventana de CA Enterprise Log Manager: 

Creación de filtros locales

Puede crear un filtro local para delimitar el ámbito de la consulta o el informe que esté viendo, o los incidentes mostrados en el área Incidentes.

Para crear filtros locales

1. Abra la consulta o el informe que desee filtrar (o haga clic en la ficha Incidentes) y haga clic en el botón Filtros locales de la parte superior del panel.

Aparece el cuadro de diálogo Filtros locales, donde se muestra la ficha Filtros rápidos.

2. (Opcional) Haga clic en la ficha Incidentes si desea filtrar los incidentes mostrados en lugar de los eventos.
3. (Opcional) Seleccione la casilla de verificación Coincidencia para introducir un valor específico mediante el cual buscar eventos o incidentes.

Nota: Puede buscar varios valores, frases o valores parciales mediante la sintaxis especializada de coincidencia.

4. Haga clic en Agregar filtro.
5. Elija el campo de eventos que quiera incluir en el filtro e introduzca el valor que debe tener el campo para que se muestre en los informes filtrados. Puede introducir valores de varias columnas volviendo a hacer clic en Agregar filtro. Si selecciona el botón Excluir, se incluyen todos los valores *excepto* el que introdujo para el nombre de campo del evento elegido.
6. (Opcional) Haga clic en la ficha Filtros avanzados para agregar más calificadores.
7. Haga clic en Guardar.

El filtro se aplica a la visualización. Puede guardar la visualización del informe definiéndola como favorita.

Edición de filtros locales

Puede editar filtros locales existentes.

Para editar filtros locales

1. Haga clic en el botón Filtros locales de la parte superior del panel de consultas o informes, o en la parte superior de la vista Incidentes.
Aparece el cuadro de diálogo Filtros locales, donde se muestra la ficha Filtros rápidos.
2. Cambie o agregue valores según sea necesario. Puede eliminar configuraciones de filtros individuales haciendo clic en el icono Suprimir situado junto a cada filtro, o eliminar un valor de coincidencia cancelando la selección de la casilla de verificación.

3. Haga clic en Guardar.

El filtro editado se aplica a la visualización.

Eliminación de filtros locales

Puede eliminar filtros locales y devolver una vista de consulta, informe o incidente a su estado anterior.

Para eliminar un filtro local, haga clic en el botón Borrar filtros locales de la parte superior de la visualización de la consulta, el informe o el incidente que esté viendo: 

Capítulo 10: Consultas e informes

Esta sección contiene los siguientes temas:

- [Acerca de las consultas y los informes](#) (en la página 278)
- [Asignación de etiquetas a tareas](#) (en la página 281)
- [Formato de fecha y hora](#) (en la página 283)
- [Visualización de consultas](#) (en la página 287)
- [Visualización de informes](#) (en la página 288)
- [Desactivación de la visualización del informe seleccionado](#) (en la página 290)
- [Ejemplo: Ejecutar informes de PCI](#) (en la página 291)
- [Peticiones](#) (en la página 296)
- [Creación de consultas](#) (en la página 313)
- [Edición de consultas](#) (en la página 331)
- [Eliminación de consultas personalizadas](#) (en la página 331)
- [Desactivación de la visualización de la consulta seleccionada](#) (en la página 332)
- [Exportación e importación de definiciones de consultas](#) (en la página 332)
- [Creación de informes](#) (en la página 335)
- [Ejemplo: Crear informes a partir de consultas existentes](#) (en la página 338)
- [Ejemplo: configuración de la federación y de los informes federados](#) (en la página 341)
- [Edición de informes](#) (en la página 346)
- [Eliminación de informes personalizados](#) (en la página 346)
- [Exportación de definiciones de informes](#) (en la página 348)
- [Importación de definiciones de informes](#) (en la página 349)
- [Preparación para el empleo de informes mediante listas con clave](#) (en la página 350)
- [Visualización de un informe mediante una lista con clave](#) (en la página 370)

Acerca de las consultas y los informes

Puede emplear las consultas de las siguientes formas:

- Puede realizar una consulta para visualizar datos de eventos o incidentes casi en tiempo real.
- Puede seleccionar un informe predefinido para visualizar los resultados de múltiples consultas relacionadas.
- Puede crear un informe formado por las consultas seleccionadas.
- Puede emplear consultas de peticiones para buscar información preseleccionada específica.
- Puede programar las consultas para ejecutarlas en datos recientes como alertas de acción que notifican a las partes responsables a través del correo electrónico. Las alertas de acción también se añaden a la fuente RSS que se puede visualizar mediante lectores de terceros.
- Puede crear sus propias consultas para visualizar, crear o generar informes de alertas de acción.

Existen dos tipos de consultas e informes:

- Las consultas e informes de *suscripción* están predefinidos por CA y se ofrecen con la aplicación de CA Enterprise Log Manager durante la instalación o se añaden con una actualización de la suscripción.
- Las consultas e informes de *usuario* son aquellos creados por un usuario. Puede crear una consulta o un informe desde el principio o puede crear uno basándose en una consulta o un informe de suscripción que desee modificar.

CA Enterprise Log Manager ofrece una lista completa de consultas e informes por suscripción. Si se le ha asignado la función Auditor, Analyst o Administrator, podrá visualizar todos los informes y consultas de suscripción. Además, puede llevar a cabo las acciones siguientes en cualquier consulta o informe de suscripción que visualice:

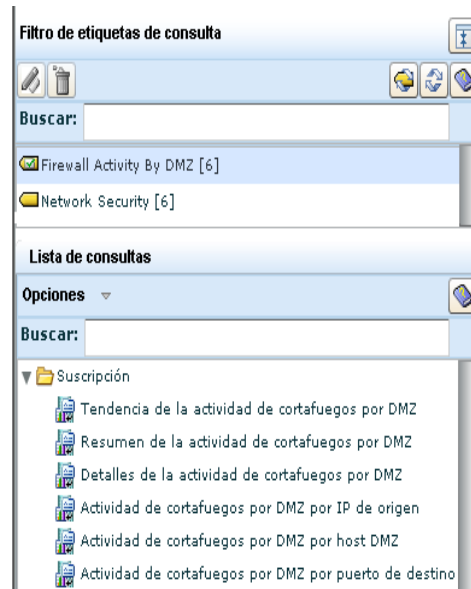
- Actualización de los datos mostrados
- Edición de los filtros locales para ocultar los datos que no desea visualizar
- Eliminación de los filtros locales para volver a mostrar la consulta o el informe sin filtrar
- Adición de la consulta o el informe mostrado a la lista de favoritos
- Impresión de consultas
- Cambio de la opción para mostrar la consulta o el informe seleccionado
- Cierre de la consulta o del informe mostrado

Sólo los usuarios a los que se les ha asignado la función Analyst o Administrator podrán llevar a cabo las acciones siguientes:

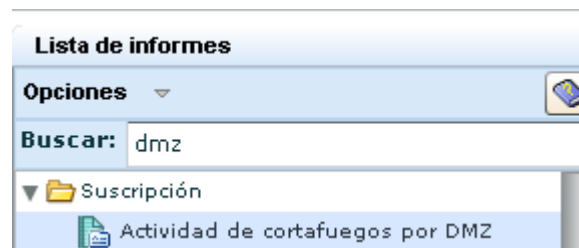
- Creación de una consulta o un informe de usuario desde el principio
- Copia de una consulta o un informe de suscripción para emplearlo como base para una consulta o un informe de usuario
- Edición de una consulta o un informe de usuario
- Exportación de una consulta o un informe de usuario
- Eliminación de una consulta o un informe de usuario
- Almacenamiento de cambios en la consulta o el informe de usuario seleccionado
- Importación de la definición de una consulta o un informe de usuario

Ejemplo de consultas e informe relacionado

Tomemos como ejemplo la etiqueta Actividad de cortafuegos por DMZ. Tenga en cuenta que está asociada a seis consultas independientes de este tema.



Las consultas que visualiza en la lista de consultas se emplean en los informes. En la ficha Informes, puede mostrar un informe denominado Actividad de cortafuegos por DMZ.



En la ilustración siguiente, sólo se muestran los nombres. Tenga en cuenta que cada nombre refleja una de las seis consultas del informe. La mayoría de los informes incluye resultados de consultas para resúmenes, tendencias y detalles.

Actividad de cortafuegos por DMZ



Asignación de etiquetas a tareas

Las etiquetas le permiten asignar categorías a los informes y a las consultas para contar con una rápida referencia, al tiempo que ofrecen un marco de trabajo organizativo para generar informes en su entorno. Las etiquetas de categorías también permiten la división sencilla de mano de obra por función o tipo de evento.

Puede usar las etiquetas predefinidas o crear sus propias etiquetas personalizadas para informes o consultas. Por ejemplo, podría crear una etiqueta "Mensual" para agregarla a los informes que quisiera programar todos los meses, con el fin de facilitar su referencia y visualización. Esto también le permitiría agregar o eliminar informes en las tareas de informes sin editar las propias tareas, simplemente agregando la etiqueta Mensual a la nueva tarea, o quitándola de una antigua.

Puede agregar etiquetas personalizadas a consultas o informes individuales como parte del proceso de creación o edición de dicha consulta o informe. Una vez que ha creado la etiqueta nueva, su nombre aparece en la lista de etiquetas y puede seleccionarla para agregarla a otros informes o consultas.

Puede cambiar el nombre o eliminar las etiquetas personalizadas. Puede eliminar etiquetas personalizadas de los informes o consultas que las incluyen mediante la edición del informe o consulta.

Capítulo 11: Formato de fecha y hora

CA Enterprise Log Manager utiliza archivos de propiedades de configuración regional diferentes para mostrar el contenido de la interfaz de usuario de una configuración regional concreta. CA Enterprise Log Manager proporciona los archivos de configuración regional siguientes en el directorio `/opt/CA/LogManager/locale`:

- `de_ui.properties`
- `en_ui.properties`
- `fr_ui.properties`
- `ja_ui.properties`
- `es_ui.properties`
- `it_ui.properties`

Estos archivos de propiedades de configuración regional se actualizan a través de las versiones, los Service Packs y las suscripciones. Se pueden utilizar para cambiar el formato de fecha y hora predeterminado a un formato deseado. El formato de fecha y hora configurado se muestra en la interfaz de usuario y en los resultados de consulta e informe.

Esta sección contiene los siguientes temas:

[Formatos de fecha y hora compatibles](#) (en la página 284)

[Cambio del formato de fecha y hora](#) (en la página 286)

Formatos de fecha y hora compatibles

CA Enterprise Log Manager admite los formatos de fecha y hora siguientes:

Letra del patrón	Descripción
Y	Indica un año. Los valores posibles son los siguientes: ■ Dos ■ Cuatro Si el número de la letra del patrón es dos, el valor se interpreta como dos dígitos. Por ejemplo, YY=11 para el año 2011. Si el número de la letra del patrón es cuatro, el valor se interpreta como cuatro dígitos. Por ejemplo, YYYY=2011.
M	Indica un mes del año. Los valores posibles son los siguientes: ■ Uno ■ Dos ■ Tres ■ Cuatro Si el número de la letra del patrón es uno, el valor se interpreta como uno o dos dígitos. Por ejemplo, M=1 o 11. Si el número de la letra del patrón es dos, el valor se interpreta como dos dígitos. Por ejemplo, MM=01. Si el número de la letra del patrón es tres, el valor se interpreta como tres letras. Por ejemplo, MMM=Ene. Si el número de la letra del patrón es cuatro, el valor se interpreta como el texto completo. Por ejemplo, MMMM=Enero.
D	Indica un día del mes. Los valores posibles son los siguientes: ■ Uno ■ Dos Si el número de la letra del patrón es uno, el valor se interpreta como uno o dos dígitos. Por ejemplo, D=1 o 11. Si el número de la letra del patrón es dos, el valor se interpreta como dos dígitos. Por ejemplo, DD=01 o 11.

Letra del patrón	Descripción
E	Indica un día de la semana. Los valores posibles son los siguientes: ■ Tres ■ Cuatro Si el número de la letra del patrón es tres, el valor se interpreta como tres letras. Por ejemplo, EEE=Lun. Si el número de la letra del patrón es cuatro, el valor se interpreta como el texto completo. Por ejemplo, EEEE=Lunes.
A	Indica un formato de hora. Los valores posibles son los siguientes: ■ AM ■ PM
J	Indica la hora en un reloj de 24 horas en el intervalo 0-23.
H	Indica la hora en un reloj de 24 horas en el intervalo 1-24.
K	Indica la hora en un reloj de 12 horas en el intervalo 0-11.
L	Indica la hora en un reloj de 12 horas en el intervalo 1-12.
N	Indica un minuto de una hora. Los valores posibles son los siguientes: ■ Uno ■ Dos Si el número de la letra del patrón es uno, el valor se interpreta como uno o dos dígitos. Por ejemplo, N=1 o 11. Si el número de la letra del patrón es dos, el valor se interpreta como dos dígitos. Por ejemplo, NN=01 o 11.
S	Indica un segundo de un minuto. El valor posible es el siguiente: ■ Dos Si el número de la letra del patrón es dos, el valor se interpreta como dos dígitos. Por ejemplo, SS=01 o 11.
Q	Indica un milisegundo de un segundo. Los valores posibles son los siguientes: ■ Dos ■ Tres Si el número de la letra del patrón es dos, el valor se interpreta como dos dígitos. Por ejemplo, QQ=01 o 11. Si el número de la letra del patrón es tres, el valor se interpreta como tres dígitos. Por ejemplo, QQQ=001.

Por ejemplo, si la fecha actual es 11 de febrero de 2011 y la hora actual es 14.20.12 en un reloj de 24 horas, la fecha y hora puede tener los formatos siguientes:

- EEEE, MMM. D, YYYY J:NN:QQQ—Viernes, Feb. 11, 2011 14:20:012
- EEEE, MMM. D, YYYY K:NN:SS A—Viernes, Feb. 11, 2011 2:20:12 PM
- DD/MM/YYYY—11/02/2011
- MM/DD/YYYY—02/11/2011

Cambio del formato de fecha y hora

Se pueden realizar los pasos siguientes para cambiar el formato de fecha y hora:

1. Cree un archivo de propiedades de configuración regional. Por ejemplo, si el idioma del explorador es inglés y desea utilizar el formato de fecha y hora de Gran Bretaña, cree un archivo de propiedades de configuración regional llamado en-GB_ui.properties.

Nota: El nombre de un archivo de propiedades de la configuración regional debe coincidir con el nombre del idioma que se muestra en los valores de configuración del idioma del explorador.

2. Copie el contenido del archivo de propiedades de configuración regional en_ui.properties en el archivo de propiedades de configuración regional en-GB_ui.properties.
3. Abra el archivo de propiedades de configuración regional en-GB_ui.properties y edite las propiedades de dateFormat y formatString.
4. Guarde los cambios.
5. Reinicie iGateway.

Nota: Se debe actualizar un archivo de propiedades de configuración regional creado con el contenido del último archivo de propiedades de configuración regional correspondiente proporcionado por CA Enterprise Log Manager. Se puede personalizar el archivo después de la actualización.

Más información:

[Formatos de fecha y hora compatibles](#) (en la página 284)

Visualización de consultas

Todos los usuarios a los que se han asignado funciones Auditor, Analyst o Administrator pueden visualizar todas las consultas. Las consultas predefinidas se listan en la carpeta Suscripción. Cuando se define la primera consulta personalizada, se añade a la lista de consultas una carpeta de usuario que contendrá la consulta personalizada. Tras ello, todas las consultas personalizadas se añaden a esta carpeta de usuario.

Para visualizar consultas

1. Haga clic en la ficha Consultas e informes y, a continuación, en la subficha Consultas.

En el panel izquierdo, aparecen el botón de maximización Filtro de etiquetas de consulta, la lista de consultas, así como el menú Opciones y un cuadro de texto de búsqueda.

2. Seleccione la consulta que desea visualizar a través de uno de los métodos siguientes:
 - Desplácese por la lista de consultas y seleccione la consulta que desee visualizar.
 - Introduzca una palabra clave en el cuadro de búsqueda para mostrar sólo las consultas que contengan la palabra coincidente en los nombres.
 - Seleccione una etiqueta mostrada o introduzca una palabra clave en el cuadro de búsqueda de etiquetas para limitar las etiquetas visualizadas. Seleccione una etiqueta para mostrar las consultas relacionadas. Seleccione la consulta que desea visualizar.
 - Si desea buscar una consulta personalizada, contraiga la carpeta Suscripción, expanda la carpeta Usuario y, a continuación, desplácese por la lista de la carpeta Usuario.

La consulta seleccionada aparece en el panel de detalles en el formato de tabla. Los resultados más recientes aparecen primero en la tabla de resultados. Para consultar los resultados adicionales, haga clic en las teclas de dirección o seleccione un intervalo de filas de la lista.

Nota: Si los resultados de consulta no se agrupan, la lista muestra los intervalos de fila que se han consultado y el intervalo secuencial siguiente que se encuentra disponible. Si los resultados de consulta se han agrupado, la lista mostrará todos los intervalos de filas disponibles en todo el conjunto de resultados.

3. (Opcional) Lleve a cabo una de las acciones siguientes:
 - Haga clic en Editar filtros locales para hacer que los filtros muestren sólo los datos que desea visualizar. Para restaurar la visualización de consultas original, haga clic en Borrar los filtros locales.
 - Haga clic en Agregar a favoritos para añadir la consulta o el informe visualizado a la lista de favoritos.
 - Haga clic en Actualizar para actualizar los datos y mostrar los añadidos más recientemente.
 - Haga clic en Imprimir para imprimir la consulta.
4. Haga clic en Cerrar para cerrar la consulta mostrada.

Visualización de informes

Todos los usuarios a los que se les ha asignado la función Auditor, Analyst o Administrator pueden visualizar todos los informes. Los informes predefinidos se listan en la carpeta Suscripción. Cuando se define el primer informe personalizado, se añade a la lista de informes una carpeta de usuario que contendrá el informe personalizado. Tras ello, todos los informes personalizados se añaden a esta carpeta de usuario.

La selección de un informe en la lista de informes ejecuta las consultas que forman el informe en entradas de registro que se encuentran actualmente en los sistemas de almacenamiento de registro de eventos internos. Los resultados del informe, que aparecen en el panel derecho, proceden de los sistemas de almacenamiento de registro de eventos del servidor de CA Enterprise Log Manager activo y de sus servidores secundarios.

Para ver informes

1. Haga clic en la ficha Consultas e informes y, a continuación, en la subficha Informes.

En el panel izquierdo, aparecen el botón de maximización Filtro de etiquetas de informe, un campo de entrada de búsqueda, la lista de informes y el menú Opciones.

2. En el menú Opciones, seleccione Mostrar informe seleccionado si no está seleccionado.

Esto le permite visualizar todos los informes seleccionados en el panel derecho.

3. Seleccione el informe que desea visualizar a través de uno de los métodos siguientes:
 - Desplácese por la lista de informes y seleccione un informe que desee visualizar.
 - Introduzca una palabra clave en el campo de búsqueda y seleccione un informe que desee visualizar en la lista filtrada
 - Haga clic en el botón de maximización para mostrar la lista de filtros de etiquetas de los informes. Seleccione una etiqueta mostrada o introduzca una palabra clave en el cuadro de búsqueda de etiquetas para limitar las etiquetas visualizadas. Seleccione una etiqueta para mostrar los informes relacionados. Seleccione el informe que desea visualizar.
 - Si desea encontrar un informe personalizado, contraiga la carpeta Suscripción, expanda la carpeta Usuario y, a continuación, desplácese por la lista de la carpeta Usuario.

El informe seleccionado aparece en el panel principal de la página.

4. (Opcional) Lleve a cabo una de las acciones siguientes:
 - Haga clic en Editar filtros locales para hacer que los filtros muestren sólo los datos que desea visualizar. Para restaurar la visualización de informes original, haga clic en Borrar los filtros locales.
 - Haga clic en Agregar a favoritos para añadir el informe visualizado a la lista de favoritos.
 - Haga clic en Actualizar para actualizar los datos y mostrar los añadidos más recientemente.
 - Haga clic en Imprimir para imprimir el informe.
5. Haga clic en Cerrar para cerrar el informe mostrado.

Desactivación de la visualización del informe seleccionado

Puede establecer la lista de informes de manera que pueda realizar cambios sin cargar los informes. Normalmente, al seleccionar un informe de la lista, éste aparece en la ventana de detalles.

La desactivación de este modo predeterminado permite ahorrar tiempo, ya que puede seleccionar un informe de la lista y editarlo de forma inmediata, sin tener que esperar a que se muestre. Esto es especialmente útil si desea editar múltiples informes y ya sabe los cambios que va a realizar.

Como los únicos usuarios que pueden crear o editar informes son los que acceden como administradores o analistas, sólo ellos podrán desactivar la opción de visualización del informe seleccionado.

Para desactivar la visualización del informe seleccionado

1. Haga clic en Opciones en la parte superior de la lista de informes.

Aparece el menú Opciones.

2. Elimine la marca de verificación situada junto a Mostrar informe seleccionado.

No se mostrará ninguno de los informes seleccionados en la lista hasta que no se vuelva a activar Mostrar informe seleccionado.

Más información

[Creación de informes](#) (en la página 335)

[Edición de informes](#) (en la página 346)

Ejemplo: Ejecutar informes de PCI

El PCI Security Standards Council es un foro global abierto responsable del desarrollo de PCI Data Security Standard (PCI DSS) que incluye requisitos para la gestión de la seguridad, las políticas y los procedimientos. Las organizaciones que almacenan, procesan o transmiten los datos de los titulares de la tarjeta deben cumplir con los 12 requisitos establecidos en PCI DSS versión 1.2.

CA Enterprise Log Manager ofrece informes de PCI predeterminados que puede visualizar en cuanto el sistema comienza a recopilar y procesar registros de eventos.

Los ejemplos que aparecen en esta sección le ayudan a familiarizarse con los informes de PCI y a aprender a programarlos y distribuirlos. Los ejemplos incluyen referencias al número asociado con el requisito de PCI DDS al que hace referencia el informe.

Más información:

[Visualización de la lista de informes mediante la etiqueta de PCI](#) (en la página 291)

[Búsqueda de informes de un control PCI DDS específico](#) (en la página 292)

Visualización de la lista de informes mediante la etiqueta de PCI

Puede comenzar la valoración de cómo emplear los informes de CA Enterprise Log Manager para demostrar la conformidad con PCI mediante la visualización de la lista de informes predefinidos con la etiqueta de PCI.

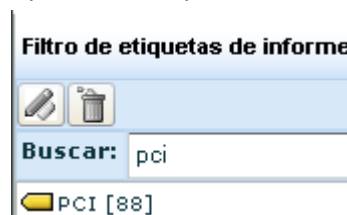
Para familiarizarse con informes que tengan la etiqueta de PCI

1. Haga clic en la ficha Consultas e informes y en la subficha Informes.

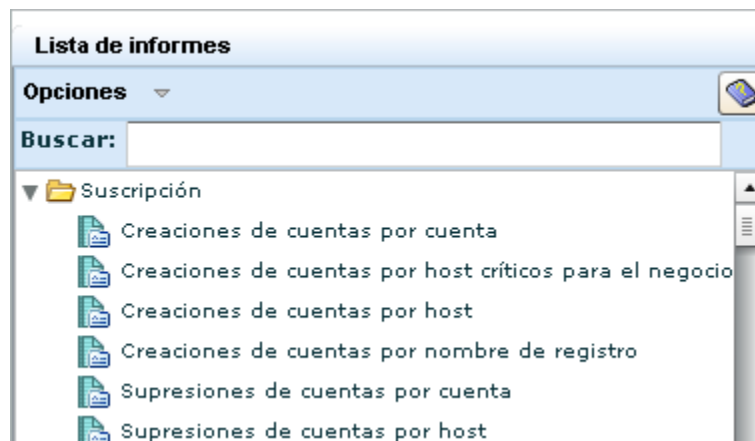
Aparecen el filtro de etiquetas de informe y la lista de informes.

2. Introduzca PCI en el campo de búsqueda de la etiqueta.

Aparece la etiqueta de PCI.



3. Revise la lista de informes asociada a la etiqueta de PCI.



Búsqueda de informes de un control PCI DDS específico

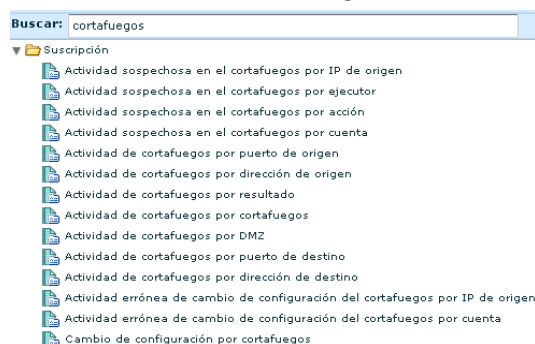
Puede buscar informes predefinidos mediante las palabras clave correspondientes a los controles PCI DDS específicos. El procedimiento siguiente muestra varios ejemplos.

Nota: Los números indicados son números asociados con el requisito de PCI DDS al que hace referencia el informe.

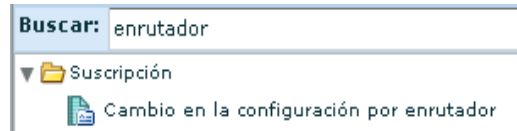
Para visualizar la lista de informes relevantes para controles PCI DDS específicos

1. Haga clic en la ficha Consultas e informes y en la subficha Informes.
2. Para localizar el informe que hace referencia a los cambios realizados en la configuración del cortafuegos (1.1.1), introduzca Cortafuegos como criterio de búsqueda.

Aparece una lista de informes parecida a la siguiente. Observe la que se denomina Cambios de configuración del cortafuegos.



3. Para encontrar el informe que hace referencia a los cambios realizados en las configuraciones de los enrutadores tras verificar la sincronización (1.3.6), introduzca Enrutador en los criterios de búsqueda.

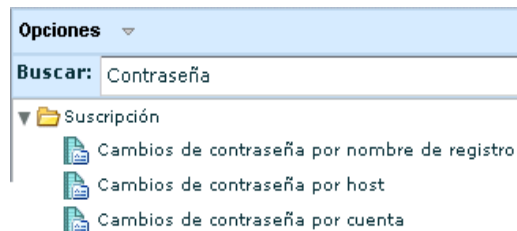


Buscar: enrutador

▼ Suscripción

- ▼ Cambio en la configuración por enrutador

4. Para encontrar los informes que hacen referencia a la gestión de contraseñas (8.5), una de las medidas de control de acceso más estrictas, introduzca Contraseña como criterio de búsqueda.



Opciones ▼

Buscar: Contraseña

▼ Suscripción

- ▼ Cambios de contraseña por nombre de registro
- ▼ Cambios de contraseña por host
- ▼ Cambios de contraseña por cuenta

5. Para encontrar los informes que hacen referencia a adiciones, modificaciones y eliminaciones en cuentas de usuario (12.5.4), una de las medidas para mantener una política de seguridad de la información, introduzca Cuenta como criterio de búsqueda.

Opciones ▾

Buscar:

▼  Suscripción

 Creaciones de cuentas por cuenta

 Creaciones de cuentas por host críticos para el negocio

 Creaciones de cuentas por host

 Creaciones de cuentas por nombre de registro

 Supresiones de cuentas por cuenta

 Supresiones de cuentas por host

 Supresiones de cuentas por nombre de registro

 Account Disable Activity on Critical Host

 Desactivaciones de cuentas por cuenta

 Desactivaciones de cuentas por host

 Desactivaciones de cuentas por nombre de registro

 Account Enable Activity on Critical Host

 Activaciones de cuentas por cuenta

 Activaciones de cuentas por host

 Activaciones de cuentas por nombre de registro

 Bloqueos de cuentas por cuenta

 Bloqueos de cuentas por host

 Bloqueos de cuentas por nombre de registro

 Gestión de cuentas por cuenta

 Gestión de cuentas por acción

 Gestión de cuentas por host

 Gestión de cuentas por nombre de registro

 Desbloques de cuentas por cuenta

 Desbloques de cuentas por host

 Desbloques de cuentas por nombre de registro

Trabajo con un único informe de PCI

Puede trabajar con cualquier informe, incluidos los informes de PCI, de estas maneras:

- Visualice el informe seleccionando el nombre del informe en la lista de informes.
- Imprima el informe.
- Programe el informe y active la opción de envío a través de correo electrónico a los destinatarios seleccionados.
- Visualice la tarea de informes programada.
- Visualice el informe generado.

Para visualizar o actuar sobre un informe seleccionado

1. Haga clic en la ficha Consultas e informes y en la subficha Informes.
2. Seleccione Mostrar informe seleccionado en la lista desplegable Opciones de la lista de informes si aún no está seleccionado.
3. Seleccione el nombre de un informe en la lista de informes.

El informe seleccionado muestra los resultados de las consultas básicas, que suelen incluir un resumen, la tendencia y detalles, así como de las consultas específicas del informe.

4. Para desactivar la carga de consultas específicas, seleccione Cancelar.



5. Para imprimir el informe visualizado, haga clic en Imprimir informe en el panel derecho.

Cuando aparezca el cuadro de diálogo de impresión, seleccione una impresora y haga clic en Imprimir.

6. Para programar la generación del informe para su visualización posterior, haga clic en Programar informe.

Aparece el asistente de programación de informes y muestra el informe en el área de informes seleccionados.

7. Introduzca el nombre de una tarea, por ejemplo, la tarea Acceso a los recursos por informe de host.

Si acepta todos los valores predeterminados, la tarea se programa para ejecutarse sin repeticiones y el informe se genera en formato PDF sin notificación a través de correo electrónico. Los datos se extraen del servidor actual, sus equivalentes federados y sus descendientes federados.

8. Haga clic en Guardar y cerrar.
9. Visualice la tarea programada. Seleccione la ficha Informes programados y, a continuación, la subficha Programación de informes.

Se muestra la tarea que acaba de programar.

Tareas programadas									
	Nombre de la tarea	Activado	Servidor	Estado	Repetición	Hora programada	Zona horaria	Creador	Formato
	Acceso a los recursos por host	verdadero	caelm2	La programación ha caducado	Ahora	Martes, 28/09/10 02:05:14	America/New_York	admin	PDF

10. Visualice el informe generado.
 - a. Seleccione la ficha Informes programados y, a continuación, la subficha Informes generados.
 - b. (Opcional) Limite las filas que se visualizan seleccionando una repetición diferente de Todos, un formato distinto a Todos, o un intervalo de tiempo correspondiente a la última hora.
 - c. (Opcional) Haga clic en Actualizar.
11. Tras revisar el informe generado, puede modificar la tarea de informe si desea generarla de forma repetida. Realice los pasos siguientes:
 - a. En la subficha Programación de informes, seleccione el informe generado y haga clic en Editar.
 - b. Seleccione el paso de programación de tareas y seleccione la opción de la frecuencia de repetición.
 - c. Haga clic en Guardar y cerrar.

Peticiones

Una petición es un tipo especial de consulta que muestra los resultados basados en el valor que ha especificado y los campos de la gramática de eventos comunes seleccionados. Sólo se devuelven filas para los eventos en los que el valor especificado aparece en uno o varios campos de la gramática de eventos comunes seleccionados.

Puede realizar cualquiera de las siguientes acciones en los resultados de consultas de peticiones:

- Seleccione Mostrar eventos sin formato para sustituir la vista de los eventos refinados con el evento sin procesar correspondiente y la hora en que se produjo.
- Especifique una cadena en el campo Coincidencia y seleccione Ir para filtrar las filas de forma que contengan los datos que coincidan con su entrada.
- Seleccione la opción Exportar datos de consulta para exportar los resultados de la consulta a un documento PDF, a una hoja de cálculo de Excel o a un archivo XML.
- Seleccione Condiciones de resultado para filtrar la vista por un intervalo de fechas especificado, establezca el límite de filas devueltas o cambie la granularidad de la hora mostrada. De forma alternativa, restablezca las condiciones de los resultados al valor predeterminado.
- Seleccione Mostrar/editar filtros locales para especificar filtros rápidos o avanzados.
- Imprima la consulta en una impresora local seleccionada.
- Actualice la información de la consulta de forma manual o seleccionando Actualización automática.

Uso de la petición del conector

Cada conector que se configure en un agente recopila eventos sin procesar de un origen de evento específico y envía los eventos al almacén de registro de eventos en un servidor de recopilación de CA Enterprise Log Manager. El proceso de refinamiento del evento convierte los eventos sin procesar en eventos refinados y los archiva en el servidor de informes de CA Enterprise Log Manager. La petición del conector realiza consultas para los eventos del servidor de informes que los conectores recopilaron como eventos sin procesar con el nombre que especifique. Los conectores pueden tener un nombre predeterminado o un nombre definido por el usuario. Copie el nombre del conector que desea utilizar y péguelo en el campo de la petición del conector; a continuación, haga clic en Ir para mostrar los resultados de la consulta de petición.

Utilice al petición del conector para:

- Ver los eventos de todos los conectores basados en la misma integración. Esto es posible si acepta el nombre de conector predeterminado al implementar conectores.
- Comprobar si un conector nuevo recupera eventos. Si varios agentes tienen conectores con el nombre que especifique, introduzca el nombre del agente en el campo Coincidencia para limitar los resultados de la consulta a los eventos que recupere el conector nuevo.

Para copiar el nombre de un conector activo

1. Haga clic en la ficha Administración.
Se mostrará la subficha Explorador de recopilación de registros.
2. Haga clic en el Explorador de agente.
Aparecerá el controlador de estado de los agentes, donde se enumeran los nombres de conectores en una columna.
3. Haga clic con el botón derecho en el conector que desee utilizar en la consulta de petición y seleccione Copiar nombre de conector.

Para utilizar la petición del conector

1. Seleccione Consultas e informes.

En la Lista de consultas se muestran las carpetas Peticiones, Suscripción y, posiblemente, Usuarios.

2. Expanda Peticiones y seleccione Conector.

En la petición Conector, se muestra el campo Conector y el siguiente campo de la gramática de eventos comunes, que debe permanecer seleccionado para que la petición funcione:

agent_connector_name

Es el nombre de un conector.

3. Haga clic con el botón derecho en el campo Conector y seleccione Pegar.

El nombre del conector que ha copiado del controlador de estado de los agentes aparece en el campo Conector.

4. Haga clic en Ir.

Aparecen los resultados de la consulta de petición del conector.

5. Utilice las siguientes descripciones para interpretar los resultados de la consulta:

Severidad de CA

Indica la severidad del evento. Los valores en orden creciente de severidad son: Información, Advertencia, Impacto menor, Impacto mayor, Crítico y Grave.

Fecha

Indica la fecha en la que se produjo el evento.

Categoría

Identifica la categoría de nivel superior de la acción del evento correspondiente. Por ejemplo, Acceso a sistema es la categoría de la acción de Autenticación.

Acción

Identifica la acción, en la que las posibles acciones se determinan en función de la clase del evento.

Agent Name

Identifica el agente en que se ejecuta el conector.

Host

Identifica el host de origen de eventos del que el conector está recopilando eventos.

Ejecutor

Identifica el actor de origen del evento, es decir, la identidad que inició la acción. El ejecutor se puede expresar como el nombre de usuario de origen o el nombre de proceso de origen.

Cuenta

Identifica el nombre de usuario de la cuenta utilizada para la autenticación cuando el conector intenta conectarse al host con el origen de eventos desde el que se recopilan los eventos sin procesar. Normalmente, se trata de una cuenta con privilegios bajos. Las credenciales de esta cuenta se configuran en el origen de evento y en el sensor de registro del conector.

Resultado

Especifica un código para el resultado del evento de la acción correspondiente: S cuando es correcto o F cuando es erróneo, o A para Aceptado, D para Eliminado, R para Rechazado y U para Desconocido.

Nombre de conector

El nombre del conector introducido en el campo de filtro de peticiones.

6. (Opcional) Seleccione Mostrar eventos sin formato.

El primer evento recopilado por un conector nuevo es para el inicio del sistema y termina con: result_string=<nombre del conector> Connector Started Successfully

Utilización de la petición de host

La petición de host realiza consultas para los eventos en los que el nombre de host especificado aparezca en los campos de la gramática de eventos comunes del evento refinado. Al refinar datos de evento sin formato, los detalles del evento pueden incluir varios nombres de host de gramática de eventos comunes diferentes. Considere este caso:

1. El iniciador del evento de `source_hostname` intenta realizar una acción, `event_action`, en un destino que reside en `dest_hostname`.

Nota: `Source_hostname` y `dest_hostname` pueden ser el mismo host o dos diferentes.

2. Este evento se registra en un repositorio en `event_source_hostname`.

Nota: `Event_source_name` puede ser un host diferente de `source_hostname` o `dest_hostname`, o una combinación de ambos.

3. Un agente de CA Enterprise Log Manager instalado en `agent_hostname` realiza una copia del evento registrado en `event_source_hostname`.

Nota: `Agent_hostname` coincide con `event_source_name` en la recopilación de registros basados en agentes, pero es diferente en la recopilación de registros directos y sin agente.

4. El agente de CA Enterprise Log Manager de `agent_hostname` transmite la copia del evento en `event_logname` a un servidor de recopilación de CA Enterprise Log Manager.

Para utilizar la petición de host

1. Seleccione Consultas e informes.

En Lista de consultas aparecen la carpeta Peticiones y una o varias carpetas para otras consultas.

2. Expanda Peticiones y seleccione Host.

Aparecerá la petición de host.

3. Escriba el nombre del host en que desea basar la consulta.

4. Seleccione los campos en los que desea realizar consultas de datos que coincidan con su entrada de nombre de host.

source_hostname

Es el nombre del host en el que se inició la acción del evento.

dest_hostname

Es el nombre de un host que actúa como destino de la acción.

event_source_hostname

Es el nombre de un host que registra el evento cuando éste tiene lugar.

Por ejemplo, puede implementar un conector basado en WinRM para que recopile eventos del Visor de eventos en un host de Windows Server 2008. Para seleccionar los eventos recuperados desde un host de Windows Server 2008, escriba el nombre de host de dicho servidor y seleccione este campo.

receiver_hostname

Coincide con agent_hostname.

agent_hostname

Es el nombre del host en el que se implementa un agente de CA Enterprise Log Manager.

5. Haga clic en Ir.

Aparecerán los resultados de la consulta de petición de host.

6. Utilice las siguientes descripciones para interpretar los resultados de la consulta:

Severidad de CA

Indica la severidad del evento. Los valores en orden creciente de severidad son: Información, Advertencia, Impacto menor, Impacto mayor, Crítico y Grave.

Fecha

Indica la fecha en la que se produjo el evento.

Usuario de origen

Identifica el nombre del usuario en source_hostname que inició la acción del evento.

Resultado

Especifica un código para el resultado del evento de la acción correspondiente: S cuando es correcto o F cuando es erróneo, o A para Aceptado, D para Eliminado, R para Rechazado y U para Desconocido.

Host de agente

Identifica el nombre del host en el que se encuentra instalado el agente de CA Enterprise Log Manager que ha recopilado el evento.

Host de receptor

Coincide con el host de agente.

Categoría

Identifica la categoría de nivel superior de la acción del evento correspondiente. Por ejemplo, Acceso a sistema es la categoría de la acción de Autenticación.

Acción

Identifica la acción del evento realizada por el usuario de origen.

Nombre de registro

Identifica el nombre de registro utilizado por el conector que recopiló el evento. Todos los conectores que se basan en la misma integración transmiten los eventos a un archivo de registro con el mismo nombre de registro.

Utilización de la petición de IP

La petición de IP realiza consultas para eventos en los que la dirección IP especificada aparezca en los campos de la gramática de eventos comunes del evento refinado. Al refinar datos de evento sin formato, los detalles del evento pueden incluir varias direcciones IP de gramática de eventos comunes diferentes. Considere este caso:

1. El iniciador del evento de `source_address` intenta realizar una acción, `event_action`, en un destino que reside en `dest_address`.

Nota: `Source_address` y `dest_address` pueden ser diferentes o coincidir.

2. Este evento se registra en un repositorio en `event_source_address`.

Nota: `Event_source_address` puede ser diferente de `source_address` o `dest_address`, o bien puede coincidir con uno o con ambos.

3. Un agente de CA Enterprise Log Manager instalado en `agent_address` crea una copia del evento registrado en `event_source_address`.

Nota: `Agent_address` coincide con `event_source_address` en la recopilación de registros basados en agentes, pero es diferente en la recopilación de registros directos y sin agente.

4. El agente de `agent_address` transmite la copia del evento de `event_logname` a un CA Enterprise Log Manager servidor de recopilación.

Para utilizar la petición de IP

1. Seleccione Consultas e informes.

En Lista de consultas aparecen la carpeta Peticiones y una o varias carpetas para otras consultas.

2. Expanda Peticiones y seleccione Host.

Aparecerá la petición de IP.

3. Introduzca la dirección IP en la que desea basar la consulta.

4. Seleccione uno o varios de los siguientes campos para realizar consultas de datos que coincidan con la entrada de dirección IP.

source_address

Es la dirección IP del host en el que se inició la acción.

dest_address

Es la dirección IP de un host que actúa como destino de la acción.

event_source_address

Es la dirección IP de un host que registra el evento sin procesar cuando éste tiene lugar.

Por ejemplo, puede implementar un conector basado en WinRM para que recopile eventos del Visor de eventos en un host de Windows Server 2008. Para seleccionar eventos recuperados desde un host de Windows Server 2008 determinado, escriba la dirección IP del servidor y seleccione este campo.

receiver_hostaddress

Coincide con agent_address.

agent_address

Es la dirección IP de un host en el que se implementa un agente de CA Enterprise Log Manager.

5. Haga clic en Ir.

Aparecerán los resultados de la consulta de la petición de IP.

6. Utilice las siguientes descripciones para interpretar los resultados de la consulta:

Severidad de CA

Indica la severidad del evento. Los valores en orden creciente de severidad son: Información, Advertencia, Impacto menor, Impacto mayor, Crítico y Grave.

Fecha

Indica la fecha en la que se produjo el evento.

Resultado

Proporciona un código para el resultado de la acción correspondiente. Las letras mostradas tienen los siguientes significados: S cuando es correcto o F cuando es erróneo, o bien A para Aceptado, D para Eliminado, R para Rechazado y U para Desconocido.

Puerto de destino

Identifica el puerto de comunicación del host de destino, el destino de la acción del evento.

IP de origen

Identifica la dirección IP desde la que se inició la acción del evento.

IP de destino

Identifica la dirección IP del host que actuó como destino de la acción del evento.

IP de origen de evento

Identifica la dirección IP del host con el repositorio en el que se registró el evento originalmente.

IP de agente

Identifica el nombre del host con el agente de CA Enterprise Log Manager responsable de la recopilación de eventos del origen de eventos.

IP de receptor

Coincide con IP de agente.

Categoría

Identifica la categoría de nivel superior de la acción del evento correspondiente. Por ejemplo, Acceso a sistema es la categoría de la acción de Autenticación.

Acción

Identifica la acción del evento.

Nombre de registro

Identifica el nombre de registro utilizado por el conector que recopiló el evento.

Utilización de la petición de nombre de registro

Los conectores que están basados en la misma integración devuelven los registros de eventos recopilados del origen de eventos al servidor de recopilación de CA Enterprise Log Manager en un archivo de registro con un nombre predefinido. La petición de nombre de registro realiza consultas para eventos que incluyan el nombre de registro que especifique.

Utilice la petición de nombre de registro para realizar consultas para eventos transferidos en un archivo de registro con el nombre especificado. Cada conector está basado en una integración. Cada integración utiliza un nombre de registro predefinido. Las consultas para un nombre de registro determinado devuelve resultados de eventos recopilados por diferentes agentes que utilizan conectores basados en la misma integración o en integraciones similares.

Se utilizan diferentes convenciones para denominar los registros:

- Nombre de integración: CA Federation es el nombre de registro de la integración CA_Federation_Manager.
- Nombre de producto: McAfee Vulnerability Manager es el nombre de registro de McAfee_VM y McAfee_VM_CM. MS AD Rights Management Services es el nombre de registro de Microsoft_Active_Directory_RMS y Microsoft_Active_Directory_RMS_ODBC.
- Nombre del proveedor: Oracle es el nombre de registro de Oracl10g, Oracle9i, Oracle_AppLog y Oracle_Syslog.
- Tipo de registro: Unix es el nombre de registro de las integraciones AIX_Syslog, HPUNIX_Syslog, Linux_Syslog, SLES_Syslog y Solaris_Syslog.

Algunos nombres de registros vuelven a usarse a medida que se agregan nuevas versiones o plataformas. Por ejemplo, NT-Security es el nombre de registro de los registros de seguridad para las integraciones NTEventLog, Windows2k8 y WinRM.

Para utilizar la petición de nombre de registro

1. Seleccione Consultas e informes.

En Lista de consultas aparecen la carpeta Peticiones y una o varias carpetas para otras consultas.

2. Expanda Peticiones y seleccione Nombre de registro.

El filtro de la petición de nombre de registro aparece con el siguiente campo:

event_logname

Es el nombre de un archivo de registro asociado con una integración específica.

3. Seleccione el nombre de registro utilizado para transmitir los eventos que desee ver y haga clic en Ir.

Aparecerán los resultados de la consulta de petición del nombre de registro.

4. Utilice las siguientes descripciones para interpretar los resultados de la consulta:

Severidad de CA

Indica la severidad del evento. Los valores en orden creciente de severidad son: Información, Advertencia, Impacto menor, Impacto mayor, Crítico y Grave.

Fecha

Indica la fecha en la que se produjo el evento.

Categoría

Identifica la categoría de nivel superior de la acción del evento correspondiente. Por ejemplo, Acceso a sistema es la categoría de la acción de Autenticación.

Acción

Identifica la acción del evento realizada por el ejecutor.

Host

Identifica el host de origen de eventos del que el conector está recopilando eventos.

Ejecutor

Identifica el actor de origen del evento, es decir, la identidad que inició la acción. El ejecutor se puede expresar como el nombre de usuario de origen o el nombre de proceso de origen.

Cuenta

Identifica al nombre de usuario de la cuenta usado para llevar a cabo la autenticación. Cuando el conector intenta establecer una conexión con el origen de evento, se produce la autenticación. La autenticación suele utilizar una cuenta con privilegios bajos. Durante la implementación del conector, el administrador configura las credenciales de esta cuenta en el origen del evento y, a continuación, identifica esta cuenta en el sensor de registro.

Resultado

Especifica un código para el resultado del evento de la acción correspondiente: S cuando es correcto o F cuando es erróneo, o A para Aceptado, D para Eliminado, R para Rechazado y U para Desconocido.

Nombre de registro

El nombre de registro introducido en el campo del filtro de petición.

Utilización de la petición de puerto

La petición de puerto realiza consultas para los eventos en los que el puerto especificado aparezca en los campos de la gramática de eventos comunes del evento refinado. Al refinar datos de evento sin formato, los detalles del evento pueden incluir varios números de puerto de gramática de eventos comunes diferentes. Considere este caso:

1. El iniciador del evento del host de origen utiliza el puerto de comunicación `source_port` saliente para iniciar la acción del evento en un destino que reside en el host de destino a través del puerto de comunicaciones `dest_port` entrante.

Nota: `Source_port` y `dest_port` coinciden para los eventos locales. De lo contrario, serán específicos del host.

2. Este evento se registra en un repositorio en el origen de evento.
3. Un agente de CA Enterprise Log Manager crea una copia del evento registrado en el origen de evento.
4. El agente transmite la copia del evento a través del puerto saliente, `receiver_port`, a un servidor de recopilación de CA Enterprise Log Manager.

Nota: El agente utiliza el puerto 17001 de forma predeterminada para establecer comunicaciones seguras con el servidor de recopilación de CA Enterprise Log Manager.

Para utilizar la petición de puerto

1. Seleccione Consultas e informes.
En Lista de consultas aparecen la carpeta Peticiones y una o varias carpetas para otras consultas.
2. Expanda Peticiones y seleccione Puerto.
Aparecerá la petición de puerto.
3. Introduzca el número de puerto en el que desea basar la consulta.
4. Seleccione los campos en los que desea realizar consultas de datos que coincidan con su entrada de número de puerto.

source_port

Es el puerto de comunicaciones utilizado para iniciar la acción.

dest_port

Es el puerto de comunicaciones en el host de destino que actúa como destino de la acción.

receiver_port

Es el puerto que el agente utiliza para comunicarse con el servidor de recopilación de CA Enterprise Log Manager.

5. Haga clic en Ir.
Aparecerán los resultados de la consulta de petición de puerto.
6. Utilice las siguientes descripciones para interpretar los resultados de la consulta:

Severidad de CA

Indica la severidad del evento. Los valores en orden creciente de severidad son: Información, Advertencia, Impacto menor, Impacto mayor, Crítico y Grave.

Fecha

Indica la fecha en la que se produjo el evento.

IP de origen

Identifica la dirección IP del host desde donde se inició la acción del evento.

Resultado

Especifica un código para el resultado del evento de la acción correspondiente: S cuando es correcto o F cuando es erróneo, o A para Aceptado, D para Eliminado, R para Rechazado y U para Desconocido.

Puerto de origen

Identifica el puerto saliente utilizado para iniciar la acción.

Puerto de destino

Identifica el puerto entrante en el host de destino.

Host de receptor

Identifica el puerto saliente del agente utilizado para enviar registros de eventos al servidor de CA Enterprise Log Manager.

Categoría

Identifica la categoría de nivel superior de la acción del evento correspondiente. Por ejemplo, Acceso a sistema es la categoría de la acción de Autenticación.

Acción

Identifica la acción del evento.

Nombre de registro

Identifica el nombre de registro utilizado por el conector que recopiló el evento.

Utilización de la petición de usuario

Cada evento expresa información acerca de dos actores: el Origen y el Destino.

- El actor Origen inicia la acción que genera el evento.

El actor Origen puede ser un usuario, `source_username`, o un proceso, `source_processname`.

- El actor Destino o "dest" es el destino de la acción.

El actor Destino puede ser un usuario, `dest_username`, o un objeto, `dest_objectname`.

La petición de usuario realiza consultas para los eventos en los que el actor especificado aparezca en los campos de la gramática de eventos comunes del evento refinado. Considere este caso:

1. El actor Origen, `source_username` o `source_processname`, intenta realizar una acción en el actor Destino, `destination_username` o `destination_objectname`.
2. Este evento se registra en un repositorio en el origen de evento.
3. Un agente de CA Enterprise Log Manager crea una copia del evento registrado en el origen del evento y la transmite al servidor de CA Enterprise Log Manager.

Para utilizar la petición de usuario

1. Seleccione Consultas e informes.
En Lista de consultas aparecen la carpeta Peticiones y una o varias carpetas para otras consultas.
2. Expanda Peticiones y seleccione Usuario.
Aparecerá la petición de usuario.
3. Escriba el nombre del usuario en que desea basar la consulta.
4. Seleccione los campos en los que desea realizar consultas de datos que coincidan con su entrada de nombre de usuario.

source_username

Es el nombre del usuario que inició la acción del evento.

dest_username

Es el nombre del usuario que actúa como destino de la acción.

source_objectname

Es el nombre del objeto implicado en la acción a la que se hace referencia en la información del evento.

dest_objectname

Es el nombre del objeto que actúa como destino de la acción.

5. Haga clic en Ir.
Aparecerán los resultados de la consulta de petición de usuario.

6. Utilice las siguientes descripciones para interpretar los resultados de la consulta:

Severidad de CA

Indica la severidad del evento. Los valores en orden creciente de severidad son: Información, Advertencia, Impacto menor, Impacto mayor, Crítico y Grave.

Fecha

Indica la fecha en la que se produjo el evento.

Host de destino

Identifica el nombre del host con el usuario que actuó como destino de la acción del evento.

Resultado

Especifica un código para el resultado del evento de la acción correspondiente: S cuando es correcto o F cuando es erróneo, o A para Aceptado, D para Eliminado, R para Rechazado y U para Desconocido.

Usuario de origen

Identifica al usuario que inició la acción del evento.

Objeto de origen

Identifica al objeto en el host de origen que estaba implicado en la acción del evento.

Usuario de destino

Identifica al usuario que actuó como destino de la acción del evento.

Objeto de destino

Identifica al objeto en el host de destino que estaba implicado en la acción del evento.

Categoría

Identifica la categoría de nivel superior de la acción del evento correspondiente. Por ejemplo, Acceso a sistema es la categoría de la acción de Autenticación.

Acción

Identifica la acción del evento.

Nombre de registro

Identifica el nombre de registro utilizado por el conector que recopiló el evento.

Creación de consultas

Pueden crear consultas personalizadas con el asistente de diseño de consulta. Cuando crea una consulta, debe elegir si se aplica a la base de datos de eventos o a la base de datos de incidentes. La base de datos de eventos de un servidor almacena información de todos los eventos que éste recibe. La base de datos de incidentes de un servidor almacena información sobre los incidentes y elementos de sus eventos de componentes, en función de lo que se especifique mediante las reglas de correlación.

También puede eliminar consultas personalizadas y exportar información sobre consultas, o copiar una consulta de suscripción para crear una consulta personalizada y, a continuación, editar dicha consulta mediante el asistente de diseño de consulta. Sólo los usuarios de tipo Administrator o Analyst pueden crear, eliminar o editar consultas.

La creación de consultas mediante el asistente de diseño de consulta consta de los pasos siguientes:

1. Apertura del asistente de diseño de consulta.
2. Agregación de detalles de identidad y etiqueta.
3. Selección de columnas de consulta.
4. (Opcional) Configuración de filtros y condiciones de consulta.
5. Configuración de intervalo de fecha y condiciones del resultado.
6. (Opcional) Elección de opciones para la visualización de consultas.
7. (Opcional) Agregación de valores de obtención de detalles para la consulta.

Más información:

[Apertura del asistente de diseño de consulta](#) (en la página 314)

[Uso de filtros avanzados](#) (en la página 509)

[Creación de visualizaciones de pantallas de consulta](#) (en la página 329)

[Adición de informes de obtención de detalles](#) (en la página 330)

Apertura del asistente de diseño de consulta

Para crear una consulta personalizada nueva, crear una copia de una consulta o editar una consulta nueva, debe abrir el asistente de diseño de consulta.

Para abrir el asistente de diseño de consulta

1. Haga clic en la ficha Consultas e informes y, a continuación, en la subficha Consultas.

Aparece la lista de consultas.

2. Haga clic en Opciones y seleccione Nuevo.

Aparece el asistente de diseño de consulta.

Al emplear el asistente:

- Haga clic en Guardar para guardar la consulta sin cerrar el asistente.
- Haga clic en Guardar y Cerrar para guardar la consulta y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Más información

[Configuración de condiciones del resultado](#) (en la página 511)

[Creación de visualizaciones de pantallas de consulta](#) (en la página 329)

[Adición de informes de obtención de detalles](#) (en la página 330)

Adición de detalles de consultas

El primer paso para crear una consulta nueva es introducir información de identificación y configurar las etiquetas que desee incluir.

Para agregar consultas nuevas

1. Abra el asistente de diseño de consulta.
2. Introduzca un nombre de consulta (obligatorio) y un nombre corto (opcional) para su empleo en los informes. El nombre corto aparece en el panel de consulta individual del informe cuando la consulta se incluye en un informe.
3. Seleccione la base de datos a la que desea aplicar su consulta:

Evento

Aplica la consulta a la base de datos de eventos, que almacena toda la información de eventos sin formato y refinados recibida por el servidor actual, o disponible a través de federación.

Incidente

Aplica la consulta a la base de datos de incidentes, que almacena los incidentes creados por el sistema de correlación de eventos y la información de eventos utilizada para crear esos incidentes. La regla de correlación establece los componentes específicos de un evento utilizados para crear un incidente y que, por ello, se almacenan en la base de datos de incidentes.

4. Introduzca las notas de diseño que desee en el campo de introducción Descripción.

Nota: Le recomendamos emplear este campo para introducir información sobre la estructura de la consulta. Por ejemplo, puede contener una explicación sobre las razones por las que la consulta contiene determinados campos y funciones.

5. Seleccione una o más etiquetas a las que desee asociar la consulta mediante el control de cambio de etiquetas.
6. (Opcional) Para agregar una etiqueta de categoría personalizada, introduzca un nombre de etiqueta en el campo de adición de etiquetas personalizadas y haga clic en el botón Agregar etiqueta.

Aparece la etiqueta personalizada, ya seleccionada, en el control de cambio de etiquetas.

7. (Opcional) Para agregar una o más etiquetas anidadas personalizadas, seleccione una etiqueta, o escriba el nombre de la etiqueta de categoría principal, seguido por una barra diagonal inversa y por el nombre de la etiqueta secundaria y, a continuación, haga clic en Agregar etiqueta. Por ejemplo, podría escribir: "Normativas\estándares del sector". Puede agregar etiquetas adicionales manteniendo el formato a\b\c...

Nota: Si suprime una de las etiquetas anidadas personalizadas, todas las etiquetas personalizadas en las cuales se anida se suprimen también, incluida la etiqueta principal. Si anida una etiqueta personalizada dentro de una etiqueta de suscripción y, a continuación, la suprime, solamente se suprimen las etiquetas personalizadas.

Cuando complete el proceso, las nuevas etiquetas aparecerán en la lista, y la etiqueta anidada personalizada estará visible al expandir la etiqueta principal.

8. Haga clic en la flecha correspondiente para avanzar al paso de diseño de consulta que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la consulta nueva aparece en la lista de consultas; si no es así, aparece el paso de diseño de consulta que haya seleccionado.

Adición de columnas de consulta

Para crear una consulta, escriba una instrucción SQL que recupere la información del evento que desee del almacén de registro de eventos. El asistente de diseño de consulta le permite automatizar este proceso.

Para crear instrucciones SQL de consultas

1. Abra el asistente de diseño de consulta.
2. Introduzca el nombre y la etiqueta, si no se han especificado aún, y vaya al paso Columnas de consulta.
3. (Opcional) Seleccione la casilla de verificación Sólo eventos únicos.
4. Especifique las columnas de gramática de eventos comunes que quiera incluir en la consulta arrastrándolos desde la lista de columnas disponibles del lado izquierdo al campo Columna del panel Columnas seleccionadas. Aparecerán en la pantalla de consultas en el orden en el que se introduzcan.

5. (Opcional) Seleccione la configuración que quiere para cada columna, incluyendo:

Mostrar nombre

Le permite introducir un nombre diferente para la columna cuando se muestra en formato de tabla o de visor de eventos. Si no introduce ningún nombre para mostrar, se emplea el nombre de campo nativo como nombre de columna; por ejemplo, "event_count".

Función

Permite aplicar una de las siguientes funciones SQL a los valores de la columna:

- COUNT: devuelve el número total de eventos.
- AVG: devuelve el promedio de los valores de event_count. Esta función sólo está disponible para campos de event_count.
- SUM: devuelve la suma de los valores de event_count. Esta función sólo está disponible para campos de event_count.
- TRIM: elimina los espacios de la cadena de texto incluida en la consulta.
- TOLOWER: convierte la cadena de texto incluida en la consulta a minúsculas.
- TOLOWER: convierte la cadena de texto incluida en la consulta a mayúsculas.
- MIN: devuelve el valor del evento más bajo.
- MAX: devuelve el valor del evento más elevado.
- UNIQUECOUNT: devuelve el número de eventos únicos.

Orden de grupo

Configura la pantalla de consulta para mostrar las columnas seleccionadas agrupadas por el atributo seleccionado. Por ejemplo, puede configurar la consulta para agrupar eventos por nombre de origen. Puede controlar el orden en que se aplica a varias columnas. Si los valores de la primera columna son idénticos, se aplicará la segunda. Por ejemplo, puede agrupar varios eventos con el mismo origen por nombre de usuario.

Orden de clasificación

Controla el orden de los valores seleccionados. Puede controlar el orden en que se aplica a varias columnas. Si los valores de la primera columna son idénticos, se aplicará la segunda.

Descendente

Define la visualización de los valores de la columna para que se muestre en orden descendente (del mayor valor al menor) en lugar de en el orden ascendente predeterminado.

No nulo

Controla si la fila se muestra en una tabla o en el visor de eventos si no contiene ningún valor. La selección de la casilla de verificación No nulo elimina la fila del resultado de la consulta si no contiene valores visualizables.

Visible

Controla si la columna es visible en formato de tabla o de visor de eventos. Puede utilizar esta configuración para hacer que los datos de la columna estén disponibles en la vista de detalles sin que aparezcan en la propia pantalla.

Nota: Si selecciona una función, excepto TRIM; TOLOWER, TOUPPER o un valor de orden de grupo para una columna, deberá utilizar el mismo valor también para el resto de columnas. En caso contrario, CA Enterprise Log Manager mostrará mensajes de error.

6. (Opcional) Utilice las flechas hacia arriba y hacia abajo situadas en la parte superior del panel Columnas seleccionadas para cambiar el orden de las columnas según sus necesidades.
7. Haga clic en la flecha correspondiente para avanzar al paso de diseño de consulta que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la consulta nueva aparece en la lista de consultas; si no es así, aparece el paso de diseño de consulta que haya seleccionado.

Configuración de filtros de consultas

Puede filtrar la información obtenida a partir de la consulta mediante filtros simples o avanzados. Los filtros simples le permiten crear instrucciones de filtros de un solo término de forma rápida y sencilla. Los filtros avanzados le permiten crear instrucciones más complejas en lenguaje SQL, incluidas instrucciones anidadas.

Para configurar filtros de consultas

1. Abra el asistente de diseño de consulta.
2. Introduzca el nombre y la etiqueta, si no se han especificado aún, y vaya al paso Filtros de consulta.

Aparece el cuadro de diálogo de filtros de consulta, donde se muestra la ficha Filtros simples.
3. Cree los filtros simples que desee para buscar los valores de campo indicados de la gramática de eventos comunes.
4. (Opcional) Haga clic en la ficha Filtros avanzados.
5. (Opcional) Cree los filtros avanzados que desee.
6. Haga clic en la flecha correspondiente para avanzar al paso de diseño de consulta que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la consulta nueva aparece en la lista de consultas; si no es así, aparece el paso de diseño de consulta que haya seleccionado.

Más información:

[Creación de un filtro de evento simple](#) (en la página 594)

[Creación de filtros de eventos avanzados](#) (en la página 597)

[Uso de filtros avanzados](#) (en la página 509)

Creación de un filtro de evento simple

Puede crear filtros simples para establecer parámetros de búsqueda de valores comunes. Por ejemplo, puede configurar el campo Modelo ideal como "Gestión de contenido" para identificar todos los eventos que tengan ese valor en el campo de la gramática de eventos comunes de Modelo ideal. Son numerosas las funciones que utilizan filtros simples, incluido las consultas de eventos e incidentes, las reglas de resumen y supresión, y las reglas de transferencia de eventos.

Para crear un filtro simple

1. Seleccione la casilla de verificación del campo o los campos de filtro simple que desee definir, y seleccione un valor en la lista desplegable, o introduzca el valor en el campo de entrada de texto.
2. Haga clic en Guardar cuando haya agregado todos los filtros simples que desee.

Más información

[Uso de filtros avanzados](#) (en la página 509)

[Creación de filtros de eventos avanzados](#) (en la página 597)

Uso de filtros avanzados

Puede utilizar filtros avanzados basados en SQL para habilitar cualquier función que consulte las bases de datos de eventos o incidentes, incluida la delimitación de consultas, o la adición de calificaciones adicionales a filtros sencillos. La interfaz Filtros avanzados le ayuda a crear la sintaxis apropiada para los filtros proporcionando un formulario para introducir columnas, operadores y valores lógicos en función de los requisitos de filtrado.

Nota: Esta sección contienen una breve descripción general de los términos SQL usados en los filtros avanzados. Para aprovechar al máximo el potencial de los filtros avanzados, debe conocer a fondo SQL y la gramática de eventos comunes.

Los siguientes términos SQL unen varias instrucciones de filtros:

And

Muestra la información del evento si *todos* los términos unidos son verdaderos.

Or

Muestra la información del evento si *cualquiera* de los términos unidos es verdadero.

Having

Restringe las condiciones de la instrucción SQL principal añadiendo una instrucción de calificación. Por ejemplo, puede definir un filtro avanzado para eventos de determinados hosts y añadir una instrucción "having" para mostrar sólo los eventos de esos host que presenten un nivel de severidad específico.

Los filtros avanzados utilizan los siguientes operadores SQL para crear las condiciones básicas:

Operadores relacionales

Incluye la información del evento si la columna tiene la relación apropiada con el valor introducido. Dispone de los siguientes operadores relacionales:

- Igual a
- Not Equal to
- Menor que
- Mayor que
- Menor o igual que
- Mayor o igual que

Por ejemplo, si usa *Greater than*, incluiría la información del evento de la columna seleccionada si su valor fuera mayor que el valor especificado.

Como

Incluye la información del evento si la columna contiene un patrón que haya introducido, usando % para definir el patrón deseado. Por ejemplo, L% devolvería cualquier valor que empezara por L, %L% devolvería cualquier valor que tuviera una L, pero no como primera o última letra.

Not like

Incluye la información del evento si la columna no contiene el patrón especificado.

In set

Incluye la información del evento si la columna contiene uno o varios valores del conjunto entrecomillado introducido. Debe separar con comas los diferentes valores del conjunto.

Not in set

Incluye la información del evento si la columna no contiene uno o varios valores del conjunto entrecomillado introducido. Debe separar con comas los diferentes valores del conjunto.

Matches

Incluye cualquier información del evento que coincida con uno o más de los caracteres introducidos, de manera que puede buscar por palabras clave.

Keyed

Incluye cualquier información del evento que se haya definido como valor clave durante la configuración del servidor de informes. Puede emplear valores clave para definir la relevancia empresarial u otros grupos organizativos.

Not Keyed

Incluye cualquier información del evento que no se haya definido como valor clave durante la configuración del servidor de informes. Puede emplear valores clave para definir la relevancia empresarial u otros grupos organizativos.

Creación de filtros de eventos avanzados

Los filtros avanzados se usan en muchas funciones, incluido la creación de consultas, la programación de informes y los filtros locales y globales.

Para crear filtros avanzados

1. Si está creando una tarea de informe programada o una tarea de alerta de acción, haga clic en la ficha Eventos o en la ficha Incidentes para establecer el tipo de filtro apropiado. Como los informes o las tareas de alerta pueden contener tanto consultas de eventos como de incidentes, se pueden establecer los tipos de filtro por separado.
2. Haga clic en Nuevo filtro de evento.
La primera fila de la tabla de filtros de eventos se activa y sus columnas Lógica y Operador se rellenan con los valores predeterminados "And" y "Equal to" respectivamente.
3. Haga clic en la celda Lógica y cambie el valor lógico según sea necesario.
4. Haga clic en la celda Columna y seleccione la columna de información del evento deseado en el menú desplegable.
5. Haga clic en la celda Operador y seleccione el operador deseado en el menú desplegable.
6. Haga clic en la celda Valor e introduzca el valor deseado.
7. (Opcional) Haga clic en las celdas de paréntesis de apertura y cierre e introduzca el número de paréntesis que necesita.
8. (Opcional) Repita los pasos de 1 a 6 según sea necesario para agregar más instrucciones de filtros.
9. Haga clic en Guardar cuando haya introducido todas las instrucciones de filtro que quiera.

Más información:

[Creación de un filtro de evento simple](#) (en la página 594)

[Uso de filtros avanzados](#) (en la página 509)

Configuración de condiciones del resultado

Puede configurar un intervalo de fechas y otras condiciones del resultado para la consulta, incluidos límites de filas y período de tiempo de base de visualización. Las condiciones del resultado se pueden modificar en cualquier momento hasta la hora de ejecución de la consulta, de manera que resultan un método útil para modificar consultas sin cambiar la consulta de base o sus filtros.

Si está creando una tarea de informe programada o una tarea de alerta de acción, puede establecer condiciones de resultado tanto para consultas de eventos como de incidentes que constituyen la tarea según sea necesario.

Puede establecer los tipos de condiciones del resultado siguientes:

- Condiciones de intervalo de fechas que controlan el período de búsqueda de la consulta
- Condiciones de visualización, como el número máximo de filas
- Condiciones de eventos agrupados, como los eventos agrupados más recientes tras una fecha determinada o los eventos agrupados que contienen un cierto número de eventos

Nota: Si no agrupa al menos una columna al crear la consulta, los usuarios no podrán editar las condiciones del resultado en la pantalla de consultas.

Establecimiento de intervalos de fecha y hora

Puede establecer una condición de intervalo de fecha y hora para su consulta. Esto mejora la eficacia de la consulta reduciendo la parte del almacenamiento del registro de eventos que debe buscar.

Puede utilizar un intervalo de tiempo predefinido, o bien crear uno personalizado. Para que el intervalo de tiempo personalizado funcione correctamente, debe establecer tanto una hora de inicio como de finalización. Si sólo establece un parámetro de hora, se expresa como una cláusula "Where" en SQL de consulta.

Para configurar condiciones de resultado

1. Abra el cuadro de diálogo de condiciones de resultados.
2. Si está creando una tarea de informe programada o una tarea de alerta de acción, haga clic en la ficha Eventos o en la ficha Incidentes para establecer el tipo de filtro apropiado. Como los informes o las tareas de alerta pueden contener tanto consultas de eventos como de incidentes, se pueden establecer los tipos de filtro por separado.
3. Seleccione un intervalo de tiempo predefinido en la lista desplegable. Por ejemplo, si desea ver los eventos recibidos el día anterior, seleccione "Día anterior".

Nota: Si está creando una alerta de acción o un informe programado, la interfaz muestra los siguientes intervalos de hora predeterminados.

- Alerta de acción: los 5 minutos anteriores
 - Informe programado: las 6 horas anteriores
4. (Opcional) Cree un intervalo de tiempo personalizado con los pasos secundarios siguientes:
 - a. Haga clic en Editar junto al campo de entrada "Tiempo de finalización dinámico" en el área Selección del intervalo de fechas. Esto le permite establecer la finalización del período que desee que busque la consulta.
Aparece el cuadro de diálogo Especificación de tiempo dinámico.
 - b. Seleccione el tiempo de referencia que servirá de base para el parámetro y haga clic en Agregar.
 - c. Seleccione el parámetro de hora que desee y haga clic en Agregar. Puede agregar varios parámetros de hora.
 - d. Cuando haya terminado de agregar parámetros, haga clic en Aceptar.

El cuadro de diálogo Especificación de tiempo dinámico se cierra y los valores que seleccione aparece en el área "Tiempo de finalización dinámico". Si usa varios parámetros, éstos forman una instrucción de hora completa y cada parámetro hace referencia al primero. Por ejemplo, si agrega "Inicio del mes" y "Día de la semana: martes", los valores en el área "Hora de finalización dinámica" finalizará la consulta el primer martes del mes.

Nota: si usa "Numero de" valores, como "Número de días" o "Número de horas", debe introducir un número *negativo* para establecer una hora pasada. Si utiliza un número positivo se establecerá una hora de finalización futura y provocará que la consulta continúe enviando resultados siempre que al menos un evento categorizado se encuentre en el almacén de registros.

Por ejemplo, si agrega los valores "ahora" y "número de minutos: 10" al área "Hora de inicio dinámica" inicia la consulta 10 minutos antes de la hora de finalización seleccionada.

- e. Repita el paso 2 en el área "Hora de inicio dinámica" para establecer el principio del período que desee que busque la consulta.

Si no introduce un intervalo de fecha, la consulta se aplica a todos los eventos en el almacén de registros. Si introduce un intervalo de fechas no válido, es posible que su consulta no devuelva resultados.

5. Haga clic en la flecha correspondiente para avanzar al paso de diseño de consulta que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la consulta nueva aparece en la lista de consultas; si no es así, aparece el paso de diseño de consulta que haya seleccionado.

Más información:

[Configuración de condiciones del resultado](#) (en la página 511)

[Establecimiento de condiciones de grupo y visualización](#) (en la página 514)

Establecimiento de condiciones de grupo y visualización

Puede establecer condiciones que permitan el control de las condiciones y visualización de consultas que busquen eventos basados en cómo se han agrupado.

Para establecer condiciones de grupo y visualización

1. Abra el cuadro de diálogo de condiciones de resultados.
2. Si está creando una tarea de informe programada o una tarea de alerta de acción, haga clic en la ficha Eventos o en la ficha Incidentes para establecer el tipo de filtro apropiado. Como las tareas de informe o de alerta pueden contener tanto consultas de eventos como de incidentes, se pueden establecer los tipos de filtro por separado.
3. Use los cuadros de diálogo Resultados para activar cualesquiera de las siguientes especificaciones de visualización:

Límite de consultas predeterminado

Este valor sólo está disponible para las alertas de acción y la programación de informes. Establece el trabajo de alerta o informe que utilizará el límite de fila de las consultas individuales del trabajo. Si se selecciona cualquier otro valor de resultado al crear un trabajo, CA Enterprise Log Manager sustituirá los límites de fila en las consultas de los componentes.

Límite de filas

Establece el número máximo de filas de eventos que muestra la consulta. Se comienza por los eventos más recientes.

Sin límite

Establece que la consulta recuperará todos los eventos que coincidan con el filtro. Esto puede incluir una gran cantidad de eventos, por lo que es recomendable planificar la consulta en consecuencia.

Mostrar otros

Indica la presencia de otros resultados que no se muestran debido al límite de filas, lo que le permite comparar los eventos seleccionados en el contexto de todos los eventos de ese tipo. Por ejemplo, si selecciona un límite de fila de 10 para la visualización del visor de eventos y selecciona que se muestren otros, los eventos superiores a 10 se muestran como una única entrada titulada Otros, que muestra los eventos restantes. Esta configuración sólo es efectiva cuando se selecciona el límite de filas.

Granularidad de tiempo

Establece el nivel de detalles del campo de período de tiempo utilizado en la pantalla de consulta.

4. Utilice Condiciones del resultado para consultar varios tipos o condiciones de eventos agrupados. Por ejemplo, podría establecer su consulta para buscar el último evento agrupado después de una fecha seleccionada o un número determinados de eventos de grupo. Un evento agrupado es un evento refinado para el que ha establecido una función y orden de grupo en el paso de creación de consulta.

Las condiciones de grupo utilizan el mismo sistema de instrucción de hora que los campos de intervalos de hora.

5. Haga clic en la flecha correspondiente para avanzar al paso de diseño de consulta que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la consulta nueva aparece en la lista de consultas; si no es así, aparece el paso de diseño de consulta que haya seleccionado.

Más información:

[Configuración de condiciones del resultado](#) (en la página 511)

Creación de visualizaciones de pantallas de consulta

Para crear nuevas pantallas de consulta, debe configurar los detalles de visualización, que controlan cómo se muestra la información del evento.

Para crear visualizaciones de pantallas de consulta

1. Abra el asistente de diseño de consulta.
2. Introduzca el nombre y la etiqueta, si no se han especificado aún, y vaya al paso Visualización.
3. Elija si quiere que la pantalla de consulta utilice un visor de eventos o un gráfico.

Si elige el visor de eventos, el paso de visualización finaliza. Las columnas de eventos aparecerán en la pantalla del visor de eventos en el orden en que las haya colocado durante el paso de construcción de columnas de consulta.

4. Si elige el gráfico, puede seleccionar uno o varios tipos de gráficos. Si selecciona varios tipos de gráficos, permite a los usuarios alternar entre ellos en la pantalla del informe. Las flechas hacia arriba y hacia abajo que aparecen junto a cada tipo controlan el orden en el que aparecen en el menú Cambiar visualización.

Nota: El formato de tabla siempre está disponible como visualización aunque no lo añada durante este paso.

5. Seleccione el evento que quiere que aparezca como eje X (horizontal) en el menú desplegable de columna, introduzca el texto de la etiqueta si quiere que aparezca alguno y seleccione una de las siguientes opciones del menú de tipo de visualización:
 - Categoría: utilice esta opción para las columnas de valores textuales o de cadenas, como `source_username`.
 - Lineal: utilice esta opción para los valores numéricos, como `event_count`. Cuando los valores estén extendidos, puede emplear la casilla de verificación Eje de logaritmo para permitir que el eje sea logarítmico.
 - Fecha/Hora: utilice esta opción para mostrar valores de tiempo en la fecha/hora local.
6. Repita el paso 4 usando los menús Valores del eje-Y para configurar las opciones de columna del eje Y (vertical), la etiqueta y el tipo.
7. Haga clic en la flecha correspondiente para avanzar al paso de diseño de consulta que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la consulta nueva aparece en la lista de consultas; si no es así, aparece el paso de diseño de consulta que haya seleccionado.

Adición de informes de obtención de detalles

Puede agregar a la consulta uno o varios informes de obtención de detalles. Los informes de obtención de detalles permiten a los usuarios hacer clic en un elemento de la pantalla de la consulta y visualizar otro informe relacionado.

Para agregar informes de obtención de detalles

1. Abra el asistente de diseño de consulta.
2. Introduzca el nombre y la etiqueta, si no se han especificado aún, y vaya al paso de obtención de detalles.
3. Haga clic en Agregar obtención de detalles.
4. Introduzca el nombre o vaya hasta el informe que desea que esté disponible como elemento de obtención de detalles.
5. Seleccione uno o varios parámetros disponibles en los que centrar el informe de obtención de detalles y trasládelos a la lista de parámetros seleccionados. Los informes de obtención de detalles emplean los parámetros seleccionados para mantener centrada la consulta.
6. Haga clic en la flecha correspondiente para avanzar al paso de diseño de consulta que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la consulta nueva aparece en la lista de consultas; si no es así, aparece el paso de diseño de consulta que haya seleccionado.

Edición de consultas

Puede editar consultas personalizadas existentes. No puede editar una consulta de suscripción; sin embargo, puede copiar una consulta de suscripción y editar la copia. Si edita una consulta, los cambios realizados afectarán a todos los informes que utilicen dicha consulta.

Para editar consultas

1. Haga clic en la ficha Consultas e informes y en la subficha Consultas.
Aparecen la lista de filtro de etiquetas de consulta y la lista de consultas.
2. Expanda la carpeta Usuario en Lista de consultas y seleccione la consulta que desea editar.
3. Haga clic en Opciones en la parte superior de la lista y seleccione Editar.
Aparece el asistente de diseño de consulta con las especificaciones de la consulta que ha seleccionado.
4. Realice los cambios deseados y haga clic en Guardar.

Eliminación de consultas personalizadas

Puede eliminar consultas personalizadas. No puede eliminar consultas de suscripción.

Para eliminar consultas

1. Seleccione la consulta que desea eliminar.
2. Haga clic en Opciones en la parte superior de la lista y seleccione Suprimir.
Aparece un cuadro de diálogo de confirmación.
3. Haga clic en Sí.
La consulta eliminada se quita de la lista de consultas.

Más información

[Desactivación de la visualización de la consulta seleccionada](#) (en la página 332)

[Edición de consultas](#) (en la página 331)

[Exportación e importación de definiciones de consultas](#) (en la página 332)

Desactivación de la visualización de la consulta seleccionada

Puede establecer la lista de consultas de manera que pueda realizar cambios sin cargar las consultas. Normalmente, al seleccionar una consulta de la lista, ésta aparece en la ventana de detalles.

La desactivación de este modo predeterminado permite ahorrar tiempo, ya que puede seleccionar una consulta de la lista y editarla de forma inmediata, sin tener que esperar a que se muestre. Esto es especialmente útil si desea editar múltiples consultas y ya sabe los cambios que va a realizar.

Nota: Como los únicos usuarios que pueden crear o editar consultas son los que acceden como administradores o analistas, sólo ellos podrán desactivar la opción de visualización de la consulta seleccionada.

Para desactivar la visualización de la consulta seleccionada

1. Haga clic en Opciones en la parte superior de la lista de consultas.

Aparece el menú Opciones.

2. Elimine la marca de verificación situada junto a Mostrar consulta seleccionada.

No se mostrará ninguna de las consultas seleccionadas en la lista hasta que no se vuelva a activar Mostrar consulta seleccionada.

Exportación e importación de definiciones de consultas

Puede exportar e importar detalles de consultas personalizadas para usarlos en otros servidores de gestión. Esto permite transferir consultas personalizadas correctas entre entornos de CA Enterprise Log Manager, o de un entorno de prueba a otro real.

Más información

[Importación de definiciones de consultas](#) (en la página 334)

[Exportación de definiciones de consultas](#) (en la página 333)

Exportación de definiciones de consultas

Puede exportar los detalles de las consultas creadas por el usuario para usarlos en otros servidores de gestión. La exportación se guarda como un archivo XML.

Para exportar los detalles de una consulta

1. Haga clic en la ficha Consultas e informes y, a continuación, en la subficha Consultas.
Aparece la lista de consultas.
2. Haga clic en Opciones en la parte superior de la lista y seleccione Exportar.
Aparece el cuadro de diálogo Exportar definiciones de consulta de usuario, donde se muestran los informes creados por el usuario que estén disponibles.
3. Seleccione las consultas que quiera exportar mediante el control de cambio y haga clic en Exportar.
Aparece un cuadro de diálogo de exportación.
4. Introduzca o vaya a la ubicación en la que quiera guardar los archivos de exportación XML y haga clic en Guardar.
Los archivos de consulta se guardan en la ubicación elegida y aparece un cuadro de diálogo de confirmación.
5. Haga clic en Aceptar y, a continuación, en Cerrar.
El cuadro de diálogo Exportar definiciones de consulta de usuario se cierra.

Más información

[Exportación e importación de definiciones de consultas](#) (en la página 332)

[Importación de definiciones de consultas](#) (en la página 334)

Importación de definiciones de consultas

Puede importar archivos XML de definición de consultas para su uso en el servidor de gestión local.

Para importar detalles de informes

1. Haga clic en la ficha Consultas e informes y, a continuación, en la subficha Consultas.
Aparece la lista de consultas.
2. Haga clic en Opciones en la parte superior de la lista y seleccione Importar.
Se abre un cuadro de diálogo de importación de archivo
3. Introduzca o vaya a la ubicación del archivo que quiera importar y haga clic en Aceptar.
Aparece la ventana Importar resultados.
4. Haga clic en Importar otro archivo para repetir el paso 3, o en Cerrar.
La ventana Importar resultados se cierra.

Más información

[Exportación e importación de definiciones de consultas](#) (en la página 332)
[Exportación de definiciones de consultas](#) (en la página 333)

Creación de informes

Puede crear informes personalizados para su entorno, tanto mediante el proceso indicado en esta sección para crear un informe totalmente nuevo, como a través de un informe predefinido empleado como plantilla. Puede ver informes personalizados o definirlos como plantillas de informes programados.

También puede editar o eliminar informes personalizados, así como exportar información de informes. Sólo puede llevar a cabo estas tareas de personalización si está conectado como Administrator o Analyst.

El proceso de creación de un informe nuevo mediante el asistente de diseño de informe se compone de los pasos siguientes:

1. Apertura del asistente de diseño de informe.
2. Adición de detalles del informe: indicación de un nombre para el informe nuevo y asignación de etiquetas de categorías.
3. Establecimiento de un diseño de informe: selección de las consultas que se incluirán en el informe y del modo de visualización.

Apertura del asistente de diseño de informe

Para crear un informe personalizado nuevo desde el principio o basado en un informe existente, debe abrir el asistente de diseño de informe.

Para abrir el asistente de diseño de informe

1. Haga clic en la ficha Consultas e informes y, a continuación, en la subficha Informes.

Aparece la lista de informes.

2. Haga clic en Opciones y, a continuación, seleccione Nuevo o Copiar.

Aparece el asistente de diseño de informe.

Al emplear el asistente:

- Haga clic en Guardar para guardar sin cerrar el asistente.
- Haga clic en Guardar y Cerrar para guardar el informe y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Adición de detalles del informe

Puede crear un informe nuevo desde el principio o a partir de una copia de un informe existente. Al crear un informe nuevo, debe nombrarlo y agregar las etiquetas personalizadas o de suscripción que desee asociar a dicho informe.

Para agregar detalles del informe

1. Abra el asistente de diseño de informe.
2. Introduzca un nombre de informe. También puede introducir información descriptiva opcional como referencia.
3. Seleccione una o varias etiquetas a las que desea asociar el informe mediante el control de cambio de etiquetas.
4. (Opcional) Para agregar una etiqueta de categoría personalizada, introduzca un nombre de etiqueta en el campo de adición de etiquetas personalizadas y haga clic en el botón Agregar etiqueta.

La etiqueta personalizada aparece tal y como figura en la lista de etiquetas seleccionadas.

5. (Opcional) Para agregar una o más etiquetas anidadas personalizadas, seleccione una etiqueta, o escriba el nombre de la etiqueta de categoría principal, seguido por una barra diagonal inversa y por el nombre de la etiqueta secundaria y, a continuación, haga clic en Agregar etiqueta. Por ejemplo, podría escribir: "Normativas\estándares del sector". Puede agregar etiquetas adicionales manteniendo el formato a\b\c...

Nota: Si suprime una de las etiquetas anidadas personalizadas, todas las etiquetas en las cuales se anida se suprimen también, incluida la etiqueta principal. Si anida una etiqueta personalizada dentro de una etiqueta de suscripción y, a continuación, la suprime, solamente se suprimen las etiquetas personalizadas.

Cuando complete el proceso, las nuevas etiquetas aparecerán en la lista, y la etiqueta anidada personalizada estará visible al expandir la etiqueta principal.

6. Vaya al paso Diseño o haga clic en Guardar y cerrar si ya se ha seleccionado al menos una consulta.

Establecimiento de diseños de informes

Puede diseñar la estructura del informe especificando el tamaño y las dimensiones de la cuadrícula y, a continuación, seleccionando las consultas que desea mostrar en cada sección de la cuadrícula.

Para establecer diseños de informes

1. Abra el asistente de diseño de informe. Si se trata de un informe nuevo, introduzca un nombre, seleccione una etiqueta y vaya al paso de diseño.
2. Seleccione o introduzca el número de filas y columnas que desea que aparezcan en el informe mediante las áreas de filas de la cuadrícula y columnas del panel de diseño del informe. Estos ajustes controlan el número de áreas de visualización de consultas que contendrá el informe. Puede incluir hasta 10 filas o columnas.

El número apropiado de filas, columnas y pantallas de consulta correspondientes aparece en el panel de diseño del informe.

Nota: Puede usar las flechas del lado derecho e inferior de las áreas de visualización de consultas individuales para expandirlas o reducirlas horizontal y verticalmente en función de sus necesidades.

3. (Opcional) Introduzca o seleccione un tamaño mínimo de píxeles para las áreas de visualización de la consulta en las áreas de anchura mínima y altura mínima.
4. Arrastre la consulta que quiera visualizar en cada área de visualización desde la lista de consultas hasta el área apropiada de diseño del informe.
5. (Opcional) Haga clic en el botón Editar de la parte superior del área de visualización de cada consulta para editar la consulta que haya colocado ahí o crear una nueva consulta personalizada.
6. Haga clic en Guardar y cerrar.

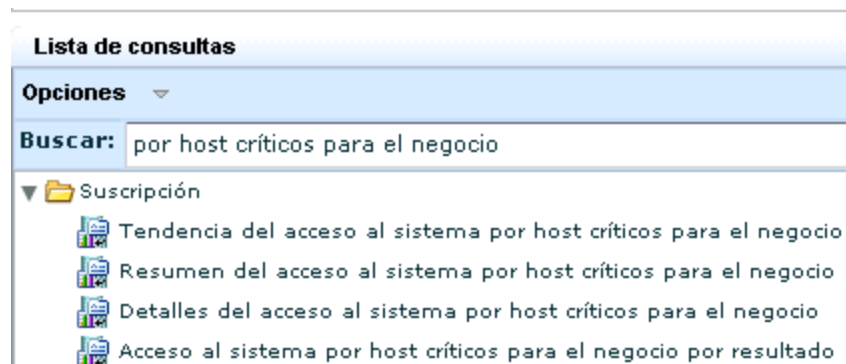
El asistente de diseño de informe se cierra. El informe nuevo aparece en la lista de informes de la carpeta Usuario.

Ejemplo: Crear informes a partir de consultas existentes

Puede crear informes personalizados compuestos por consultas predefinidas y adaptarlos a sus especificaciones.

Para crear informes a partir de consultas existentes

1. Identifique las consultas que desea incluir en el informe personalizado.
 - a. Haga clic en la ficha Consultas e informes y en la subficha Consultas si no aparece.
 - b. Introduzca una palabra o una frase clave en el campo Buscar para mostrar las consultas con el contenido a partir del que desea realizar la selección. Por ejemplo, introduzca la tendencia de host críticos.
 - c. Anote los nombres de las consultas que desea incluir en el informe personalizado. Por ejemplo, puede definir un informe de las tendencias asociadas a los host críticos para el negocio de entre los que se muestran en la ilustración siguiente, por ejemplo, los correspondientes al acceso al sistema, al acceso a los recursos y a creaciones de cuentas.



2. Para la primera consulta que desea incluir en el informe, cree una copia y agregue una etiqueta personalizada.
 - a. Seleccione una consulta y seleccione Copiar en la lista desplegable Opciones.
 - b. Cambie el nombre de la consulta e introduzca una etiqueta personalizada para agregarla. Por ejemplo, cambie el nombre de Copia de Tendencia del acceso al sistema por host críticos para el negocio por Tendencia del acceso al sistema por host críticos para el negocio personalizada.

- c. Agregue una etiqueta personalizada. Por ejemplo, introduzca Tendencia_activos_críticos y haga clic en Agregar etiqueta.

- d. Haga clic en el botón de desplazamiento para mover la etiqueta preseleccionada al área de etiquetas disponibles. Por ejemplo, desplace el acceso al sistema. La única etiqueta seleccionada es la que ha añadido.

- e. Haga clic en Guardar y cerrar.
3. Para las demás consultas que desea incluir en el informe, cree una copia y seleccione la etiqueta personalizada que ha creado.
- Seleccione una consulta y seleccione Copiar en la lista desplegable Opciones.
 - Cambie el nombre de la consulta y seleccione la nueva etiqueta personalizada. Por ejemplo, cambie el nombre de Copia de Tendencia del acceso al recurso por host críticos para el negocio por Tendencia del acceso al recurso por host críticos para el negocio personalizada, desplace Tendencia_activos_críticos a la lista Etiquetas seleccionadas y elimine la etiqueta preseleccionada.
 - Haga clic en Guardar y cerrar.

Las consultas copiadas se muestran en Usuario:

4. Si las consultas se asocian a una lista con clave, defina los valores de dicha lista con clave.
5. Inicie el proceso de creación de informes del modo siguiente:
 - a. Haga clic en la ficha Consultas e informes y, a continuación, en la subficha Informes.
 - b. Seleccione Nuevo en el menú desplegable Opciones de la lista de informes.

Aparece el asistente de diseño de informe.

Agregue la etiqueta personalizada, Tendencia_activos_críticos.
6. Establezca el diseño del informe.

Diseño de informe

Arrastre y suelte consultas de la Biblioteca de consultas de la izquierda manualmente. El botón Editar le permite modificar una consulta existente.

Filas de la cuadrícula: 3 **Columnas:** 1

Custom Account Creations by Business Critical Hosts Trend
Custom Account Creations by Business Critical Hosts Trend

Custom Resource Access by Business Critical Hosts Trend
Custom Resource Access by Business Critical Hosts Trend

Custom System Access by Business Critical Hosts Trend
Custom System Access by Business Critical Hosts Trend

7. Haga clic en Guardar y cerrar.
8. Planifique el informe en función de la etiqueta personalizada que ha creado.
9. Visualice el informe.

Nota: Es conveniente examinar todos los informes nuevos para comprobar que ofrecen la información deseada del modo más adecuado posible.

Ejemplo: configuración de la federación y de los informes federados

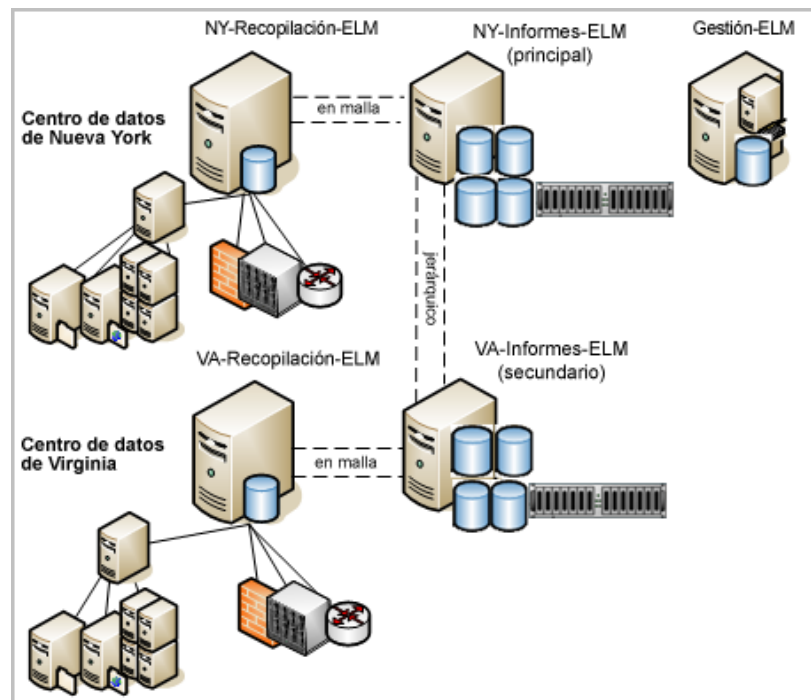
Puede recopilar registros de centros de datos separados geográficamente y con un gran volumen y establecer la generación de informes de manera que los datos distribuidos reciban consultas de uno solo de los centros de datos.

Observe un caso de ejemplo en el que los dos centros de datos de gran volumen están ubicados en Nueva York y en Virginia, con las oficinas centrales en Nueva York. Cada centro de datos cuenta con un servidor de recopilación que recopila y procesa los registros de eventos entrantes y los envía a su servidor de informes. El servidor de informes gestiona consultas, alertas e informes. La mayor parte de las consultas, las alertas y los informes se realiza sobre datos de eventos recopilados mediante agentes; la consolidación de datos de estos recursos de eventos requiere una federación entre los servidores de informes y los servidores de recopilación.

Algunas consultas, alertas e informes se realizan sobre eventos autocontrolados generados por servidores de CA Enterprise Log Manager; la consolidación de este tipo de datos requiere la inclusión del servidor de gestión en la federación. Si no desea consolidar datos de eventos autocontrolados, el servidor de gestión puede excluirse de la federación. Los eventos autocontrolados de este servidor se pueden controlar mediante informes locales no federados. Para facilitar el uso, el servidor de gestión está excluido de esta federación; la inclusión podría realizarse creando una federación en malla entre NY-Informes-ELM y Gestión-ELM.

Los nombres de los servidores son los siguientes:

- Gestión-ELM
- NY-Recopilación-ELM
- NY-Informes-ELM
- VA-Recopilación-ELM
- VA-Informes-ELM



Supongamos que el administrador de Nueva York quiere que todos los informes y alertas ejecutados desde el emplazamiento de Nueva York incluyan los datos del emplazamiento de Virginia, pero quiere que todos los informes y alertas ejecutados desde el emplazamiento de Virginia sólo incluyan los datos recopilados de forma local.

En el ejemplo siguiente, se indica cómo federar los servidores y configurar la generación de informes para cumplir los criterios de este caso. En este ejemplo, no se incluyen los procedimientos de almacenamiento automático, pero dicho almacenamiento debe configurarse para cualquier arquitectura de gran volumen.

1. Inicio sesión en un CA Enterprise Log Manager con credenciales de administrador.
2. Haga clic en la ficha Administración y seleccione la subficha Servicios.
3. Cree una federación jerárquica en la que NY-Informes-ELM sea el servidor principal y VA-Informes-ELM sea el servidor secundario. Para ello, siga estos pasos:
 - a. Expanda el servicio de almacenamiento de registro de eventos y, a continuación, seleccione el nombre del servidor que será el servidor principal en la federación jerárquica, en este caso, NY-Informes-ELM.



- b. Seleccione VA-Informes-ELM en la lista de servidores secundarios disponibles de la federación y desplácelo a la lista seleccionada.



4. Cree una federación en malla entre NY-Informes-ELM y NY-Recopilación-ELM en la que cada uno de ellos sea un servidor secundario del otro. Para ello, siga estos pasos:
 - a. Seleccione el servidor NY-Informes-ELM en la lista de almacenamiento de registro de eventos.
 - b. Seleccione NY-Recopilación-ELM entre los servidores secundarios disponibles de la federación y desplácelo a la lista seleccionada.
 - c. Seleccione el servidor NY-Recopilación-ELM en la lista de almacenamiento de registro de eventos.
 - d. Seleccione NY-Informes-ELM entre los servidores secundarios disponibles de la federación y desplácelo a la lista seleccionada.
5. Cree una federación en malla entre VA-Informes-ELM y VA-Recopilación-ELM en la que cada uno de ellos sea un servidor secundario del otro. Para ello siga estos pasos:
 - a. Seleccione el servidor VA-Informes-ELM en la lista de almacenamiento de registro de eventos.
 - b. Seleccione VA-Recopilación-ELM entre los servidores secundarios disponibles de la federación y desplácelo a la lista seleccionada.
 - c. Seleccione el servidor VA-Recopilación-ELM en la lista de almacenamiento de registro de eventos.
 - d. Seleccione VA-Informes-ELM entre los servidores secundarios disponibles de la federación y desplácelo a la lista seleccionada.
6. Configure los ajustes del servidor de informes global y las anulaciones de los ajustes locales de VA-Informes-ELM como se detalla a continuación. Los servidores distanciados geográficamente suelen emplear servidores de correo diferentes.
 - a. Seleccione Servidor de alertas en la lista de servicios.
 - b. Configure los valores de configuración locales y globales según sea necesario para la opciones del servidor de correo desde el nodo NY-Informes-ELM.
 - c. Si desea enviar por correo electrónico los informes, seleccione el servidor de informes y, a continuación, el nodo NY-Informes-ELM.
 - d. Establezca las opciones del formato PDF locales o globales, o las opciones del informe relacionadas con la retención de informes y alertas.

7. Para cada informe programado para ejecutarse desde NY-Informes-ELM, lleve a cabo lo siguiente:
 - a. Seleccione la ficha Informes programados y la ficha Programación de informes.
 - b. Haga clic en Programar un informe.
 - c. Seleccione el informe que desea programar y realice los pasos 2, 3, 4 y 5 según proceda.
 - d. Haga clic en el paso Selección de servidores, seleccione NY-Informes-ELM en la lista de servidores disponibles y desplácelo a la lista de servidores seleccionados. A continuación, acepte el valor predeterminado (Sí) para la consulta federada.
 - e. Haga clic en Guardar y cerrar.

1 2 3 4 5 6

Selección de informes Filtros de informe Condiciones de resultado Programar tareas Destino Selección de servidores

• = Requerido Zona horaria: (GMT+05:30) Asia/Calcutta

Selección de servidores

Programe los servidores y seleccione si desea consultar la federación del servidor.

Servidor	Consulta federada
NY-Reporting-ELM	Sí
	No

Los informes resultantes incluyen datos de NY-Informes-ELM, su servidor equivalente, NY-Recopilación-ELM, su servidor secundario, VA-Informes-ELM y su servidor equivalente secundario, VA-Recopilación-ELM.

Nota: La ejecución de una consulta federada desde VA-Informes-ELM incluye datos de VA-Informes-ELM y su equivalente, VA-Recopilación-ELM. No incluye datos de NY-Informes-ELM, ya que este servidor es su servidor principal en la federación jerárquica.

Edición de informes

Puede editar informes personalizados.

Nota: Puede desactivar la opción Mostrar informe seleccionado al editar varios informes. Esto le permite seleccionar y editar informes sin esperar a que aparezcan en el panel de detalles.

Para editar informes

1. Seleccione el informe que desee editar en la lista de informes.
2. Haga clic en Opciones en la parte superior de la lista y seleccione Editar.
Aparece el asistente de diseño de informe con las especificaciones del informe que ha seleccionado.
3. Realice los cambios deseados y, a continuación, haga clic en Guardar y cerrar.

El informe editado aparece en la lista de informes de la carpeta Usuario.

Eliminación de informes personalizados

Puede eliminar los informes personalizados. No puede eliminar los informes de suscripción.

Para eliminar informes personalizados

1. Haga clic en el informe personalizado que desee eliminar de la lista de informes.
2. Haga clic en Opciones en la parte superior de la lista y seleccione Suprimir.
Aparece un cuadro de diálogo de confirmación.
3. Haga clic en Sí.

El informe eliminado se quita de la lista de informes.

Más información

[Creación de informes](#) (en la página 335)

[Edición de informes](#) (en la página 346)

Ejemplo: Eliminar informes diarios con más de 30 días de antigüedad

Puede implementar políticas sobre la retención de informes mediante la configuración global de los servidores de informes. Puede establecer una política de retención diferente para cada repetición del informe programado, es decir:

- Retención de informes de una sola vez
- Retención de informes diarios
- Retención de informes semanales
- Retención de informes mensuales
- Retención de informes anuales

Debe modificar la opción predeterminada No ejecutar nunca de la utilidad de retención de informes y sustituirla por una frecuencia. Asegúrese de que la frecuencia que establece para la ejecución de la utilidad es la suficiente como para realizar las eliminaciones con la frecuencia configurada. Por ejemplo, si desea eliminar los informes diarios 1 día después de su ejecución y programa la ejecución de los informes diarios a las 6:00 h y a las 18:00 h, deberá establecer que la utilidad de retención de informes se ejecute cada 12 horas como mínimo.

Ejemplo: Eliminar todos los informes diarios con más de 30 días de antigüedad

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.

La lista de servicios muestra los servicios por servicio.

2. Haga clic en Servidores de informes.

Aparece el servidor de informes de la configuración del servicio global.

3. Siga estas directrices para llevar a cabo la configuración:

- Para automatizar la eliminación de todos los informes diarios 30 días después de su generación, establezca que la retención de informes diarios se elimine tras 30 días.
- Asegúrese de que define la frecuencia de ejecución de la utilidad de retención de informes cada número de horas, días o semanas especificado.

Utilidad de retención de informes:	☐ No ejecutar nunca	Retención de informes de una sola vez:	☐ No suprimir nunca
	☒ Ejecutar tras 1 Día(s)		☒ Suprimir tras 6 Mes(es)
Retención de informes diarios:	☐ No suprimir nunca	Retención de informes semanales:	☐ No suprimir nunca
	☒ Suprimir tras 30 Día(s)		☒ Suprimir tras 4 Semana(s)
Retención de informes mensuales:	☐ No suprimir nunca	Retención de informes anuales:	☒ No suprimir nunca
	☒ Suprimir tras 12 Mes(es)		☐ Suprimir tras 1 Día(s)

4. Haga clic en Guardar.

Exportación de definiciones de informes

Puede exportar los detalles de los archivos creados por el usuario para usarlos en otros servidores de gestión. La exportación se guarda como un archivo XML. La definición de un informe exportado incluye las definiciones de todas las consultas de dicho informe.

Para exportar los detalles de un informe

1. Haga clic en la ficha Consultas e informes y, a continuación, en la subficha Informes.

Aparece la lista de informes.

2. Haga clic en Opciones en la parte superior de la lista y seleccione Exportar.

Aparece el cuadro de diálogo Exportar definiciones de usuario, donde se muestran los informes creados por el usuario que estén disponibles.

3. Seleccione el informe o los informes que quiera exportar mediante el control de cambio y haga clic en Exportar.

Aparece un cuadro de diálogo de exportación.

4. Introduzca o vaya a la ubicación en la que quiera guardar los archivos de exportación XML y haga clic en Guardar.

Los archivos de Informe se guardan en la ubicación elegida y aparece un cuadro de diálogo de confirmación.

5. Haga clic en Aceptar y, a continuación, en Cerrar.

El cuadro de diálogo Exportar definiciones del informe de usuario se cierra.

Más información

[Importación de definiciones de informes](#) (en la página 349)

Importación de definiciones de informes

Puede importar archivos XML de definición de informes para su uso en el servidor de gestión local.

Para importar detalles de informes

1. Haga clic en la ficha Consultas e informes y, a continuación, en la subficha Informes.

Aparece la lista de informes.

2. Haga clic en Opciones en la parte superior de la lista y seleccione Importar.
Se abre un cuadro de diálogo de importación de archivo

3. Introduzca o vaya a la ubicación del archivo que quiera importar y haga clic en Aceptar.

Aparece la ventana Importar resultados.

4. Haga clic en Importar otro archivo para repetir el paso 3, o haga clic en Cerrar.

La ventana Importar definiciones de consulta e informe de usuario se cierra.

Más información

[Exportación de definiciones de informes](#) (en la página 348)

Preparación para el empleo de informes mediante listas con clave

Todos los informes se crean a partir de una o varias consultas. Algunas consultas que se utilizan en los informes predefinidos están diseñadas para seleccionar todos los valores de una tabla determinada en la que un campo de atributo contiene un valor utilizado como criterio para compilar la lista de valores de clave. Por ejemplo, una tabla de activos tiene un campo denominado `IsCritical`. Una consulta que seleccione todos los nombres de activos de la tabla de activos en los que `IsCritical` sea igual a `Sí`, sólo seleccionará los nombres de los activos críticos. Estos nombres se podrían devolver a CA Enterprise Log Manager para actualizar los valores de la clave `Critical_Assets`.

La preparación para utilizar informes predefinidos con listas con clave implica las tareas siguientes:

- (Opcional) Activación de la importación de valores dinámicos, si se utiliza CA IT PAM.
- Creación de listas con clave para las claves predefinidas que no tengan valores predefinidos.
- Personalización de listas con clave para las claves predefinidas que tengan valores predefinidos.
- Mantenimiento de las listas con clave utilizadas en los informes predefinidos que desee utilizar. Actualice la lista con clave con los valores actuales.

Además, puede agregar nuevas claves para los informes personalizados que utilicen listas con clave y, a continuación, agregar valores para cada nueva clave. También puede agregar valores a las claves `Business_Critical_Sources` y `ELM_System_Lognames` para las consultas a petición que diseñe usted mismo.

Activación de la importación de valores dinámicos

Los procedimientos necesarios para activar la importación de valores dinámicos sólo se aplican a los usuarios de CA IT PAM.

Si utiliza CA IT PAM y dispone de tablas u hojas de cálculo en las que conserva listas de archivos, bases de datos, hosts y usuarios, puede aprovechar estos datos. Puede crear un proceso que lea la tabla o el archivo, seleccione los valores correspondientes a la clave y devuelva estos valores a la lista de valores de CA Enterprise Log Manager para esa clave.

Para importar valores dinámicos

1. Cree un proceso en CA IT PAM para cada uno de los valores de clave que desee generar a petición.

Nota: Si algún proceso lee una tabla de base de datos, instale un agente de CA IT PAM en el servidor con la base de datos de SQL Server 2005.

2. Configure la integración de CA IT PAM para valores dinámicos en CA Enterprise Log Manager.

Más información:

[Creación de un proceso de CA IT PAM para generar una lista de valores](#) (en la página 352)

[Configuración de la integración de CA IT PAM para valores dinámicos](#) (en la página 353)

Acerca de los procesos de valores dinámicos

Un proceso de valor dinámico es un proceso de CA IT PAM que se puede invocar para rellenar o actualizar la lista de valores para una clave seleccionada que se utiliza en los informes o las alertas. Se supone que ya está almacenando listas principales de los archivos, las bases de datos, los host, los usuarios, etc., que forman el entorno de trabajo y que esta lista principal está diseñada con atributos que permiten realizar consultas sobre los conjuntos de valores que le interesan. Si utiliza CA IT PAM, puede crear procesos que se invoquen para ejecutar consultas que devuelvan los datos a CA Enterprise Log Manager para utilizarlos como valores de clave en los informes y las alertas basados en claves. La posibilidad de crear una lista de valores de forma dinámica es un método muy útil para mantener la lista de claves volátiles actualizada con los valores actuales.

Creación de un proceso de CA IT PAM para generar una lista de valores

Puede crear un proceso en CA IT PAM para cada lista de valores de clave que desee generar a petición. Para obtener más información sobre la creación de procesos, utilice la documentación de CA IT PAM. Todos los procesos deben cumplir los requisitos de CA Enterprise Log Manager relacionados con InputKey, los parámetros del proceso local ValueList y FaultString, así como los operadores de cálculo Correcto y Error.

Siga estas directrices:

- El proceso debe aceptar la clave seleccionada como InputKey.
 - El proceso debe definir los dos parámetros siguientes del proceso local:
 - ValueList recupera la lista de valores.
 - FaultString recupera la cadena de error.
- Nota:** CA Enterprise Log Manager necesita los nombres exactos de estos parámetros para utilizarlos como parámetros de la interfaz de salida.
- El proceso debe contener los dos operadores de cálculo siguientes:
 - Operador de cálculo Correcto: Process.ValueList =<variable que contiene una lista de valores separados por comas>
 - Operador de cálculo Error: Process.FaultString =<variable que contiene un mensaje de error>

Si crea un script, tenga en cuenta estas directrices adicionales:

- Si su script selecciona columnas de una tabla de base de datos, deberá existir un agente de IT PAM en el servidor en el que esté instalado SQL Server 2005. Los servidores SQL deben aparecer en su dominio, dentro de Todos los puntos de contacto. El servidor SQL que contenga datos de clave deberá mostrar el nombre de agente para el servidor SQL.
- El script incorporado debe ejecutar la utilidad sqlcmd para recuperar la lista deseada.

Más información:

[Configuración de la integración de CA IT PAM para valores dinámicos](#) (en la página 353)

Configuración de la integración de CA IT PAM para valores dinámicos

La integración de CA IT PAM se puede configurar para optimizar uno de los tipos siguientes de procesos de CA IT PAM o ambos:

- Proceso de salida de alerta/evento: un proceso que invoca el procesamiento de un sistema de terceros como, por ejemplo, un producto de departamento de asistencia técnica.
- Proceso de valores dinámicos: un proceso que acepta una clave de entrada y devuelve valores actuales para esa clave como un archivo de valores separados por comas (*.csv).

La configuración para cualquiera de los fines requiere capacidad para iniciar e iniciar sesión en CA IT PAM. Recopile los siguientes valores:

- Nombre de host completo o dirección IP del servidor de CA IT PAM.
- Puerto (el valor predeterminado es 8080).
- Nombre de usuario y contraseña que CA Enterprise Log Manager utilizará para iniciar sesión en CA IT PAM

La configuración de CA IT PAM para valores dinámicos permite importar la lista de valores que se genera dinámicamente mediante el proceso de valor dinámicos configurado. La importación se realiza al configurar o actualizar los valores con clave en determinados informes y alertas.

El procedimiento siguiente se refiere tanto a la configuración común como a la específica para los valores dinámicos.

Para configurar la integración de CA IT PAM para el proceso de valores dinámicos

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Haga clic en Servidores de informes.
Aparece el servidor de informes de la configuración del servicio global.
3. Desplácese al área de IT PAM.
4. Cree las entradas siguientes para activar el acceso a CA IT PAM:
 - a. Introduzca el nombre de host completo del servidor en el que esté instalado CA IT PAM.
 - b. Acepte el número de puerto predeterminado 8080.
 - c. Introduzca las credenciales válidas para CA IT PAM.
5. Introduzca una ruta de proceso en el campo Proceso de valores dinámicos.
Esta ruta de proceso se convierte en la predeterminada al importar valores dinámicos.
6. Haga clic en Guardar.
Aparecerá el mensaje siguiente: Confirmación: Los cambios en la configuración se han guardado correctamente.

Enfoques para el mantenimiento de listas con clave

Las listas con clave se utilizan en algunos informes predefinidos y en determinadas consultas predefinidas etiquetadas como apropiadas para las alertas de acción. Si piensa utilizar estos informes o crear alertas que utilicen estas consultas, puede utilizar cualquier combinación de los siguientes enfoques para mantener las listas con clave.

- Puede agregar valores de clave directamente para cualquier clave seleccionada. También puede seleccionar un valor de clave y editarlo o suprimirlo.
- Es posible importar valores de clave almacenados en una lista CSV. O puede exportar la lista de valores actual como un archivo CSV, actualizar ese archivo y, a continuación, importar el archivo cargado para que rellene la lista de valores.
- Puede ejecutar un proceso de CA IT PAM que genere de forma dinámica una lista actual y devuelva los valores como un archivo CSV que rellene la lista de valores.

Si desea crear informes personalizados que utilicen una lista con clave, puede agregar una clave personalizada y, a continuación, agregar o importar sus valores.

Puede identificar una o varias listas con clave en una consulta y, a continuación, actualizar esa lista antes de programar un informe o una alerta que incluya esa consulta.

Más información:

[Actualización manual de una lista con clave](#) (en la página 358)

[Actualización de una lista con clave con exportación/importación](#) (en la página 359)

[Ejemplo: actualización de una lista con clave con un archivo CSV](#) (en la página 361)

[Utilización de consultas etiquetadas como alertas de acción](#) (en la página 373)

Creación de una lista con claves

Las listas con claves le permiten crear un grupo y asignarle valores. Por tanto, puede consultar el nombre del grupo y cualquiera de los valores en el grupo devolverá un resultado positivo. Puede asignar valores de forma individual o importarlos desde un archivo .csv. Puede crear listas con claves personalizadas o agregar valores a listas predefinidas.

Por ejemplo, algunas consultas para informes de concesión de privilegios buscan un valor clave denominado "Privileged_Groups". Cuando una consulta incluye este valor, obtiene todas las filas en las que ese campo contiene alguno de los valores especificados en el grupo.

Para crear una lista con claves

1. Haga clic en la ficha Administración, en la subficha Biblioteca y en la carpeta Lista con claves.
2. Haga clic en Nuevo para una nueva lista, o seleccione la lista a la que desee agregar valores.

Los detalles de la lista con clave aparecerán en el panel derecho.

3. Escriba un nombre y una descripción para la lista con claves, y seleccione un tipo.
4. Introduzca el proceso de valores dinámicos de CA IT PAM que genera valores para la clave seleccionada.

Nota: El proceso de valores dinámicos de CA IT PAM solamente actualiza la lista de usuarios de la tabla de valores de la lista de claves. La lista de usuarios se sobrescribe periódicamente con los últimos valores.

5. (Opcional) Si desea comprobar la validez del proceso de valores dinámicos de IT PAM introducido, haga clic en el icono de prueba.

Si la conexión es correcta, aparecerá un mensaje de confirmación.

6. Si desea importar valores, vaya al paso 10. Si desea agregar valores de forma individual, vaya al paso 7.
7. Haga clic en Agregar en la parte superior de la tabla Valores de la lista con claves.
Aparecerá una fila resaltada en la columna Usuario.
8. Haga clic en la fila y escriba un valor.
9. Repita los pasos 6-7 para agregar valores adicionales.

10. Haga clic en Importar en la parte superior del área Detalles de la lista, busque el archivo que contiene los valores que desee importar, y haga clic en Aceptar.

Los valores aparecen en el área de valores.

Nota: Sólo puede importar archivos .csv que no contienen caracteres especiales.

11. Cuando haya agregado todos los servicios que desee, haga clic en Guardar. La nueva lista aparecerá en la carpeta Usuario de la carpeta de Listas con claves.

Actualización manual de una lista con clave

Existen varias formas de actualizar los valores de una lista con clave. Una de ellas consiste en agregar, editar y suprimir los valores manualmente.

Para actualizar de forma manual una lista con clave

1. Haga clic en la ficha Administración, en la subficha Biblioteca y en la carpeta Lista con claves.
2. Expanda la carpeta Lista con claves y seleccione la lista con clave que desea actualizar.
3. Para agregar un valor a la lista con clave:
 - a. Seleccione la clave a la que desee agregar un valor.
 - b. Haga clic en Agregar valor.
 - c. Introduzca el nombre del valor en el campo Nombre y haga clic en Aceptar.

El valor agregado aparecerá en la lista de valores de la clave seleccionada.
 - d. Repita estos pasos con todos los valores que desee agregar.
4. Para suprimir un valor de una lista con clave:
 - a. Seleccione una clave con un valor que no sea necesario.
 - b. Seleccione el valor que desee suprimir y haga clic en Eliminar valor.

Aparecerá un mensaje de confirmación.
 - c. Haga clic en OK.

El valor se suprimirá de la lista de valores de la clave seleccionada.
 - d. Repita estos pasos con todos los valores que desee suprimir.
5. Para editar un valor de la lista con clave:
 - a. Seleccione la clave con el valor que desee modificar.
 - b. Seleccione el valor que desee modificar y haga clic en Editar valor.
 - c. Edite la entrada en el campo Nombre y haga clic en Aceptar.

El valor aparecerá en la lista de valores de la clave seleccionada con el nombre modificado.
 - d. Repita estos pasos con todos los valores que desee editar.
6. Haga clic en Guardar.

Se actualizarán los valores de las claves seleccionadas.

Actualización de una lista con clave con exportación/importación

Si almacena valores que correspondan a una clave en una hoja de cálculo de Excel, puede guardar la hoja de cálculo como una lista de valores separados por comas (*.csv) y rellenar la lista con clave para los valores seleccionados con una importación.

Los valores de la lista con clave se pueden actualizar en un archivo CSV como se indica a continuación:

- Si el archivo CSV contiene valores actuales para una clave determinada y la lista de valores que se muestra no está actualizada, puede importar los valores directamente del archivo CSV.
- Si desea crear un archivo CSV o actualizar un archivo con valores obsoletos, utilice una secuencia exportación, edición, importación.

Para actualizar una lista con clave con exportación o importación

1. Haga clic en la ficha Administración, en la subficha Biblioteca y en la carpeta Lista con claves.
2. Expanda la carpeta Lista con claves y seleccione la lista con clave que desea actualizar.
3. Para actualizar los valores de una clave seleccionada desde un archivo CSV que contenga valores actuales:
 - a. Seleccione la clave en la lista Valores de clave que desee actualizar.
 - b. Haga clic en Importar valores en la barra de herramienta de la lista de valores.

Aparecerá el cuadro de diálogo Importar archivo.
 - c. Haga clic en Examinar y desplácese hasta la ubicación en la que se encuentre el archivo CSV que contenga la clave seleccionada.
 - d. Seleccione el archivo para importar, haga clic en Abrir y haga clic en Aceptar.

La lista de valores se actualizará con los valores del archivo CSV.

4. Para actualizar los valores para una clave seleccionada en la que el archivo CSV no exista o no esté actualizado:
 - a. Seleccione la clave en la lista Valores de clave que desee actualizar.
 - b. En la barra de herramientas Valores, haga clic en Exportar valores, vaya a la ubicación donde desea guardar el archivo CSV y haga clic en Guardar.

Aparecerá un mensaje de confirmación de acción correcta.
 - c. Haga clic en OK.
 - d. Vaya al archivo exportado, abra la hoja de cálculo y modifique o suprima las columnas presentes como necesario. Desplácese para mostrar la última columna y agregue nuevas entradas. A continuación, guarde el archivo como un archivo CSV.
 - e. Seleccione la misma clave y haga clic en Importar valores.
 - f. Haga clic en Examinar, seleccione el archivo que ha guardado y haga clic en Abrir.
 - g. Haga clic en OK.

El archivo se carga. Puede desplazarse a la parte inferior de la lista de valores para confirmar que la entrada nueva está incluida.

Ejemplo: actualización de una lista con clave con un archivo CSV

Para proporcionar valores a las listas con clave, puede utilizar los tres métodos siguientes:

- Introduzca los valores de clave manualmente
- Importación de los valores clave desde un archivo CSV
- Importación de valores de clave desde un proceso de CA IT PAM especificado

Utilice el ejemplo siguiente como guía para actualizar los valores de una lista con clave definida por el usuario en la que los valores se almacenen en una hoja de cálculo de Excel que se guardará como una lista de valores separados por comas (*.csv).

Para actualizar una lista con clave con un archivo CSV

1. Haga clic en la ficha Administración, en la subficha Biblioteca y en la carpeta Lista con claves.
2. Expanda la carpeta de Lista con claves, seleccione la lista con clave que desea actualizar, como Cuentas_predeterminadas, y haga clic en Exportar valores.

Aparecerá el cuadro de diálogo Exportar con el nombre de archivo predeterminado file.csv.
3. Seleccione el directorio en el que desea guardar el archivo exportado. Introduzca el nombre del archivo, por ejemplo, Cuentas_predeterminadas.csv, y haga clic en Guardar.

Aparecerá un mensaje de confirmación.
4. Haga clic en OK.
5. Abra el archivo .csv exportado, desplácese hasta la última columna y agregue la entrada que desea incluir. Opcionalmente, también puede eliminar la columna de cualquier entrada predeterminada que desee retirar de la lista con claves de Cuentas_predeterminadas.
6. Guarde y cierre el archivo .csv y vuelva a la interfaz de CA Enterprise Log Manager.
7. Haga clic en Importar valores para la lista que desea actualizar, como la lista de claves Cuentas_predeterminadas.

8. Haga clic en Examinar, seleccione el archivo que ha guardado y haga clic en Abrir.
9. Haga clic en OK.

El archivo se carga. Puede desplazarse hasta la parte inferior de la lista Valores para confirmar que la entrada nueva está incluida.

Actualización de una lista con clave con un proceso de valores dinámicos

Si utiliza procesos de CA IT PAM para generar una lista de valores asociados con una clave utilizada en las consultas de CA Enterprise Log Manager, ejecute el proceso de valores dinámicos de IT PAM desde CA Enterprise Log Manager y actualice los valores de una clave determinada. La importación le permite ahorrar tiempo al no tener que introducir manualmente todos los valores de una clave determinada. Si cambian los valores de una de las claves, puede actualizarlos en CA Enterprise Log Manager, seleccionando la clave y repitiendo la importación de los valores dinámicos.

Configure la integración de CA IT PAM para valores dinámicos antes de intentar importar valores de lista con clave desde CA IT PAM.

Para importar valores para una lista con clave desde CA IT PAM

1. Haga clic en la ficha Administración, en la subficha Biblioteca y en la carpeta Lista con claves.
2. Expanda la carpeta Lista con claves y seleccione la lista con clave que desea actualizar.
3. Para crear una clave para los valores que se vayan a importar:
 - a. Haga clic en Agregar en la parte superior de la tabla de valores con clave.
Se seleccionará la primera fila disponible en la columna Usuario.
 - b. Haga clic en la fila y escriba el nombre de la nueva clave.
 - c. Haga clic en Guardar.
4. Para actualizar los valores dinámicos de una clave existente:
 - a. Seleccione la clave.
 - b. Haga clic en Importar lista de valores dinámicos en la parte superior del panel de detalles.
Aparecerá el cuadro de diálogo Importar lista de valores dinámicos.
 - c. Introduzca el nombre del proceso de valores dinámicos de IT PAM que genere los valores para la clave seleccionada y, a continuación, haga clic en Aceptar.
Se ejecutará el proceso de CA IT PAM asociado, se devolverá un archivo con los resultados y se actualizarán los valores de la clave seleccionada.
 - d. Haga clic en Guardar.

Más información:

[Activación de la importación de valores dinámicos](#) (en la página 351)

[Acerca de los procesos de valores dinámicos](#) (en la página 351)

[Creación de un proceso de CA IT PAM para generar una lista de valores](#) (en la página 352)

[Configuración de la integración de CA IT PAM para valores dinámicos](#) (en la página 353)

Determinación del uso de la lista de con clave para una consulta

Se recomienda mantener actualizadas las listas con claves con los valores actuales. Para actualizar una lista con clave de una alerta o un informe determinado, en primer lugar identifique las consultas utilizadas en el informe o la alerta. A continuación, determine la lista con clave utilizada en la consulta de origen o la consulta. Con frecuencia, las consultas que utilizan listas con clave hacen referencia al nombre de la lista con clave en el nombre de la consulta. Por ejemplo, existen consultas con "Cuentas predeterminadas" o "Grupo con privilegios" en el nombre de la consulta.

Determinación del uso de la lista con claves para una consulta

1. Abra una copia de la consulta que se desea comprobar en busca del uso de una lista con claves en el asistente de diseño de consulta.
2. Haga clic en el paso Filtros de consulta y, a continuación, en la ficha Filtros avanzados.
3. Una consulta que emplea una lista con clave tiene un filtro con el operador con clave. El valor es el nombre de la lista con claves, por ejemplo, Cuentas_predeterminadas.
4. Haga clic en Cancelar. No se guardará la copia de la consulta.

Creación de valores con clave para informes predefinidos

Algunas claves predefinidas que se utilizan en los informes predefinidos no tienen valores predefinidos. Para emplear estos informes de forma eficaz, debe ofrecer valores para las respectivas listas con clave. Se pueden agregar también valores personalizados a las listas con claves *con* valores predeterminados.

Las siguientes listas con claves no tienen valores predeterminados:

- Critical_Assets
- DMZ_Hosts
- EPHI_Database
- Business_Critical_Sources

Se pueden agregar valores a cualquier listas con clave manualmente o por importación.

Más información:

[Actualización manual de una lista con clave](#) (en la página 358)

[Actualización de una lista con clave con exportación/importación](#) (en la página 359)

[Ejemplo: actualización de una lista con clave con un archivo CSV](#) (en la página 361)

Creación de valores con clave para Critical_Assets

Este tema proporciona un ejemplo de cómo agregar valores personalizados a una lista con claves que no tenga ninguno asignado de forma predeterminada. Se puede seguir este ejemplo para agregar valores a otras listas con claves existentes.

Puede emplear determinados informes y consultas para controlar las actividades de los host críticos para el negocio. Para ello, primero debe identificar estos host como valores en la lista clave-valor de Critical_Assets.

Los siguientes Informes utilizan la lista Critical_Assets:

- Creaciones de cuentas por host críticos para el negocio
- Inicio de sesión erróneo en host críticos para el negocio
- Sesiones de acceso a los recursos por host críticos para el negocio
- Acceso a los recursos por host críticos para el negocio
- Acceso al sistema por host críticos para el negocio

Informes parecidos para CA Access Control, CA Identity Manager y CA SiteMinder utilizan la lista con clave Critical_Assets, por ejemplo: CA Access Control - Creaciones de cuentas por host críticos para el negocio.

Las siguientes consultas utilizan la lista Critical_Assets:

- (>5) Inicios de sesión por cuentas de admin. en sistemas críticos durante la noche para como mínimo 1 día
- (>5) Inicios de sesión por cuentas de admin. en sistemas críticos durante los fines de semana para como mínimo 1 semana
- Actividad de excepción del sistema

Si crea una consulta personalizada en los activos críticos, defina el filtro como se indica a continuación:

Columna	Operador	Valor
dest_hostname	Keyed	Critical_Assets

Para definir un filtro para otras listas con claves, sustituya el valor por el valor de lista que desee. Por ejemplo, se puede establecer el valor de filtro de EPHI_Database para filtrar por nombres de host que pertenezcan a esa lista con claves.

Para crear valores con clave para Critical_Assets

1. Haga clic en la ficha Administración, en la subficha Biblioteca y en la carpeta Lista con claves.
2. Expanda la carpeta de Lista de Clave, y seleccione Critical_Assets.
3. Lleve a cabo una de las acciones siguientes para crear esta lista:
 - Haga clic en Agregar valor e introduzca cada valor nuevo que desee incluir en la lista con clave.
 - Cree una hoja de datos de Excel con una fila, en la que cada columna sea un valor. Guárdela como un archivo csv. Haga clic en Importar valores para importar la lista editada.
 - Si los valores para esta clave se generan de forma dinámica mediante el proceso de valores dinámicos de CA IT PAM, haga clic en Importar lista de valores dinámicos.
4. Haga clic en Guardar.

Los informes que utilicen esta lista con clave y se hayan generado mediante tareas programadas comenzarán a reflejar datos para los valores actualizados.

Personalización de valores con clave para Administrators

Este tema proporciona un ejemplo de cómo agregar valores personalizados a una lista con claves predeterminada que tenga algunos valores ya establecidos. Se puede seguir este ejemplo para agregar valores a otras listas con claves existentes.

Puede emplear informes predefinidos y sus consultas asociadas para controlar las actividades de los administradores. Los valores predefinidos incluyen Administrator, root, sa y admin. Para personalizar la lista, identifique otras cuentas del entorno que tengan valores de privilegios de administrador en la lista de valores de clave para Administrador.

Si crea una consulta personalizada que utilice esta clave, defina el filtro como se indica a continuación:

Columna	Operador	Valor
dest_username	Keyed	Administradores

Para definir un filtro para otras listas con claves, sustituya el valor por el valor de lista que desee. Por ejemplo, se puede establecer el valor de filtro de EPHI_Database para filtrar por nombres de host que pertenezcan a esa lista con claves.

Para personalizar valores con clave para administradores

1. Haga clic en la ficha Administración, en la subficha Biblioteca y en la carpeta Lista con claves.

En la parte inferior del panel principal, se muestra una lista de claves a la que debe añadir valores definidos por el usuario.

2. Seleccione la clave, Administrators.

Aparecen los valores predefinidos.

3. Lleve a cabo una o varias de las acciones siguientes para actualizar esta lista:

- Actualice la lista manualmente:
 - Haga clic en Agregar valor e introduzca un valor nuevo que desee incluir en la lista con clave.
 - Seleccione un valor y haga clic en Eliminar valor para suprimir el valor de la lista.
 - Seleccione un valor, haga clic en Editar valor, modifíquelo y haga clic en Aceptar.
- Actualice la lista con exportación/importación:
 - a. Haga clic en Exportar valores para exportar la lista actual.
 - b. Abra la lista exportada, édítela para cambiar los valores y guarde el archivo.
 - c. Haga clic en Importar valores para importar la lista editada.
- Haga clic en Importar valores para importar los valores en un archivo csv actualizado.
- Si los valores para esta clave se generan dinámicamente mediante el proceso de valores dinámicos de CA IT PAM configurado, haga clic en Importar lista de valores dinámicos.

4. Haga clic en Guardar.

Los informes que utilicen esta lista con clave y se hayan generado mediante tareas programadas comenzarán a reflejar datos para los valores actualizados.

Visualización de un informe mediante una lista con clave

Los resultados de un informe se pueden ver antes de que se programe su generación. Algunos informes predefinidos utilizan listas con clave en las que la clave está predefinida pero los valores están definidos por el usuario. Cuando se agregan o se importan valores para una clave, se recomienda ver el informe mediante la lista con clave.

Para ver un informe mediante una lista con clave

1. Haga clic en la ficha Consultas e informes y en la subficha Informes.
2. Seleccione un informe que utilice una lista con clave.
3. Vea los resultados.

Capítulo 12: Alertas de acción

Esta sección contiene los siguientes temas:

[Acerca de las alertas de acción](#) (en la página 372)

[Utilización de consultas etiquetadas como alertas de acción](#) (en la página 373)

[Identificación de otras consultas que se pueden utilizar para las alertas](#) (en la página 375)

[Personalización de consultas para las alertas de acción](#) (en la página 376)

[Consideraciones de las alertas de acción](#) (en la página 388)

[Trabajo con procesos de salida de alerta/evento de CA IT PAM](#) (en la página 391)

[Trabajo con mensajes SNMP](#) (en la página 429)

[Creación de alertas de acción](#) (en la página 475)

[Ejemplo: Crear una alerta de acción para el espacio en disco bajo](#) (en la página 486)

[Ejemplo: Crear una alerta para un evento autocontrolado](#) (en la página 490)

[Ejemplo: Envío de un correo electrónico al Administrator cuando se detiene el flujo de eventos](#) (en la página 493)

[Configuración de retenciones de alertas de acción](#) (en la página 496)

[Ejemplo: Crear una alerta para Business Critical Sources](#) (en la página 497)

[Edición de alertas de acciones](#) (en la página 499)

[Activación o desactivación de alertas de acción](#) (en la página 500)

[Eliminación de alertas de acciones](#) (en la página 501)

Acerca de las alertas de acción

Las alertas de acción son informes especializados que generan un evento cuando se cumplen las condiciones de la consulta. Pueden ayudarle a controlar el entorno, ya que permiten generar notificaciones automáticas para una amplia variedad de situaciones y repeticiones. Por ejemplo, puede definir alertas de acción para enviar información de tendencias de los eventos, controlar el uso del espacio en disco o enviar notificaciones cuando se superan los umbrales de acceso erróneo.

Las alertas de acción son un buen método para cribar las grandes cantidades de datos recopilados y encontrar los pocos eventos sobre los que desea actuar ahora mismo. Puede emplear alertas de acción para notificarle sobre casi cualquier cosa que ocurra en la red de recopilación de registros. Puede crear alertas para estar informado sobre picos de tráfico entrante o saliente, tráfico en puertos determinados, acceso de determinados recursos con privilegios, cambios en la configuración de diversas entidades de red como cortafuegos, bases de datos o servidores de claves, etc.

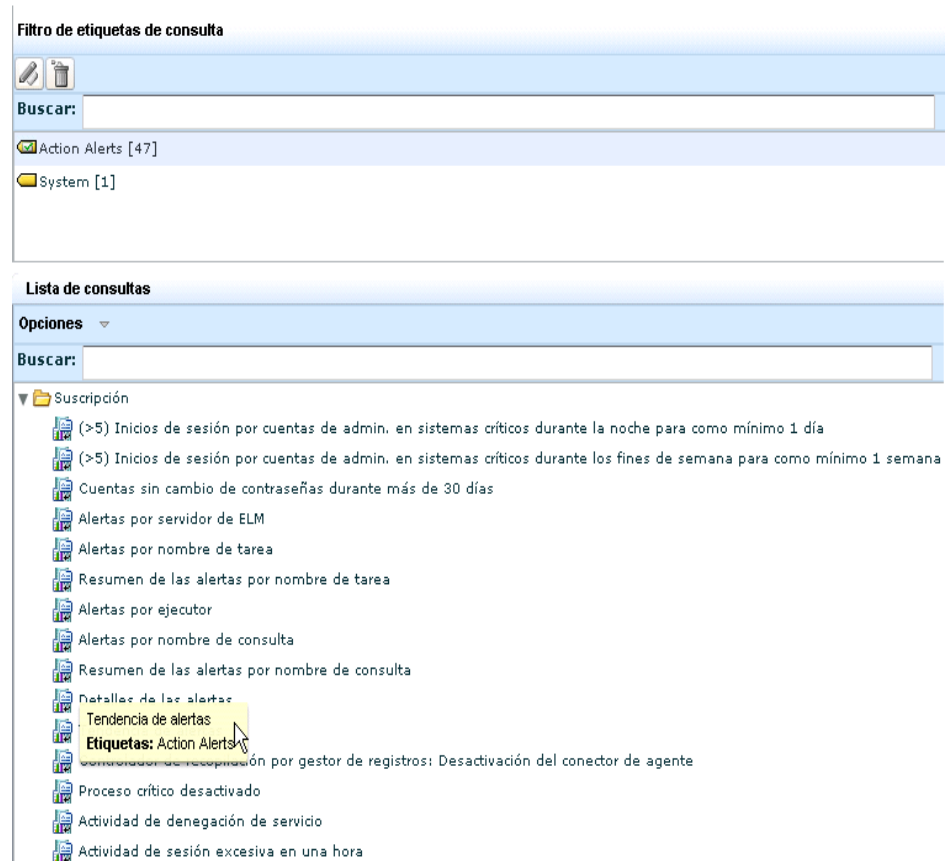
Puede crear alertas de acción de las formas siguientes:

- Mediante el asistente de alertas de acción
- Desde la pantalla de una consulta
- Mediante una consulta creada de forma personalizada

La programación de opciones es una parte importante de la creación de alertas, para que pueda controlar la duración y la frecuencia de ejecución de la tarea de alerta.

Utilización de consultas etiquetadas como alertas de acción

CA Enterprise Log Manager ofrece un determinado número de consultas con la etiqueta Alertas de acción. Para ver una lista de las consultas etiquetadas como alertas de acción, haga clic en la ficha Consultas e informes, haga clic en la subficha Consultas y seleccione la etiqueta Alertas de acción. Las consultas con esta etiqueta aparecen en la lista de consultas. Cuando desplaza el cursor sobre el nombre de una consulta, se muestran sus etiquetas.



Antes de programar las alertas de acción de estas consultas, puede obtener más información acerca del comportamiento de estas consultas. Para ver la descripción y los detalles de una consulta como Espacio en disco disponible bajo, seleccione dicha consulta en la lista de consultas y, a continuación, coloque el cursor sobre el nombre de la consulta.

Aparece un resumen de la consulta que incluye una descripción, los filtros y las condiciones de la consulta.

Espacio en disco disponible bajo

☐ Mostrar ev

Descripción: Notifica cuando el espacio en disco disponible se encuentra a menos del 20%

Versión: 12.0.5002.0

Tags: Action Alerts

Query Last Refreshed at: Tue Sep 29 2009 10:02:46 am

Profile Filters:

Filtros globales:
Last 6 hours
From: Tue Sep 29 2009 04:02:45 AM
To: Tue Sep 29 2009 10:02:45 AM

Local Filters:
AND event_trend GREATER 80
AND receiver_name EQUAL SystemStatus
AND dest_objectclass EQUAL Disk space

Query Conditions:
event_category: Operational Security

Result conditions:
Con por lo menos 1 eventos agrupados
Zona horaria local: America/New_York

Execution time: .077 segundos

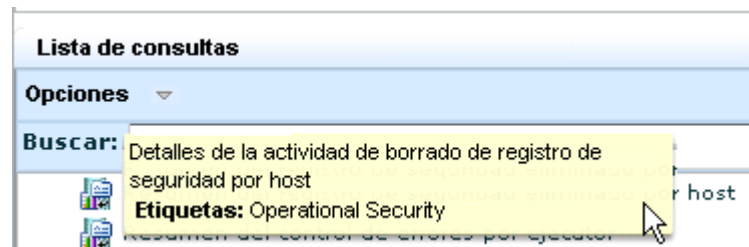
Puede programar la consulta tal y como es o puede copiar la consulta con un nombre nuevo y personalizarla según sus requisitos. Por ejemplo, puede generar una alerta cuando el espacio disponible en disco es inferior al 25 por ciento en lugar del 20 por ciento. Puede crear una consulta definida por el usuario basándose en la consulta predefinida y, a continuación, seleccionarla para su alerta de acción.

Nota: Antes de emplear las consultas en el grupo con privilegios o la cuenta predeterminada del título, puede añadir sus propios valores con clave para las listas con clave correspondientes.

Identificación de otras consultas que se pueden utilizar para las alertas

Existen consultas que no están etiquetadas como alertas de acción y que son idóneas para su inclusión en una alerta de acción programada porque sólo recuperan eventos evaluados como graves.

Por ejemplo, Detalles del registro de seguridad eliminado por host recupera todos los eventos en los que la acción de evento sea Eliminar de registro de seguridad. La única etiqueta para esta consulta es Seguridad operativa.



La acción Eliminar registro de seguridad se muestra en la gramática de eventos comunes. La gramática de eventos comunes define los dos tipos de eventos siguientes con un nivel de seguridad asignado en 6, es decir, grave.

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Seguridad operacional	Actividad de registro de seguridad	Supresión de registro de seguridad	Correcto	6
Seguridad operacional	Actividad de registro de seguridad	Supresión de registro de seguridad	Incorrecto	6

Es recomendable programar una alerta con esta consulta.

Más información:

[Identificación del filtro simple para eventos graves](#) (en la página 377)

Personalización de consultas para las alertas de acción

Las alertas están diseñadas para notificar a la persona, el proceso o el producto apropiado que se ha producido un evento grave. Al tratar de identificar consultas para basar en ellas las alertas, tenga en cuenta las consultas diseñadas para recuperar eventos con un alto nivel de seguridad.

Después de identificar definiciones para eventos graves, puede identificar las consultas que recuperarán los eventos graves. Si no existen consultas, puede crearlas.

Observe el proceso siguiente:

1. Identifique los tipos de eventos que CA considera muy graves, en los que los tipos de eventos se definen por categoría, clase, acción y resultado.
2. Identifique consultas predefinidas que estén diseñadas para recuperar sólo esta clase de eventos.
3. Identifique consultas predefinidas que estén diseñadas para recuperar eventos que puedan incluir eventos graves pero que se podrían personalizar para incluir sólo eventos graves.
4. Cree consultas personalizadas cuando no existan consultas predefinidas.
5. Programe alertas para ejecutar estas consultas con frecuencia.

Más información:

[Identificación del filtro simple para eventos graves](#) (en la página 377)

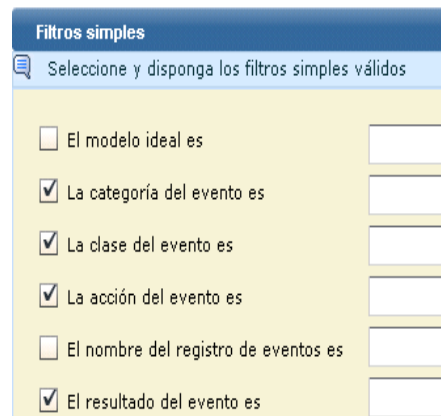
[Personalización de consultas para recuperar sólo eventos graves](#) (en la página 381)

[Creación de una consulta para recuperar sólo eventos graves](#) (en la página 379)

Identificación del filtro simple para eventos graves

La severidad de los eventos oscila entre informativa y grave. CA asigna un valor comprendido entre 2 y 7 para indicar la gravedad de los eventos basada en el modelo de gramática de eventos comunes de categoría, clase, acción y resultado. La severidad 7 se asigna a eventos de cierre del sistema. La severidad 6 se asigna a eventos con una implicación de seguridad importante o que necesiten una atención inmediata.

Si piensa crear consultas personalizadas o personalizar consultas predefinidas para utilizarlas en alertas, se recomienda examinar las definiciones del modelo de gramática de eventos comunes de los tipos de eventos graves. La definición del modelo es la base de los filtros simples. Es decir, puede crear consultas que recuperen eventos basados en la especificación de su categoría de evento, clase de evento, acción de evento y resultado de evento.



Filtros simples	
Seleccione y disponga los filtros simples válidos	
☐ El modelo ideal es	
☒ La categoría del evento es	
☒ La clase del evento es	
☒ La acción del evento es	
☐ El nombre del registro de eventos es	
☒ El resultado del evento es	

Para identificar el filtro simple para eventos graves

1. Haga clic en el vínculo Ayuda.
2. Expanda Gramática de eventos comunes y seleccione Asignación de nivel de seguridad.
3. Copie la tabla en una hoja de cálculo y ordénela por nivel de seguridad, del más alto al más bajo.

En la tabla resultante se mostrarán los tipos de eventos, comenzando con el más grave en función de la asignación de nivel de seguridad de CA.

A continuación, se muestra un ejemplo: Los resultados se reflejarán en las definiciones actuales de la gramática de eventos comunes.

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Seguridad operacional	Actividad del sistema	Cierre del sistema	Correcto	7
Seguridad operacional	Actividad del sistema	Cierre del sistema	Incorrecto	7
Gestión de configuraciones	Gestión de configuraciones	Error de configuración	Correcto	6
Acceso a datos	Gestión de objetos	Creación de archivo de control	Correcto	6
Seguridad de host	Actividad del antivirus	Error de análisis	Correcto	6
Seguridad de host	Actividad del antivirus	Eliminación de virus	Incorrecto	6
Seguridad de host	Actividad del antivirus	Detección de virus	Correcto	6
Seguridad de host	Actividad del antivirus	Cuarentena de virus	Incorrecto	6
Seguridad de host	Actividad de IDS/IPS	Infracción de firmas	Correcto	6
Seguridad de red	Actividad de infracción de firmas	Infracción de firmas	Correcto	6
Seguridad operacional	Actividad del sistema	Inicio del sistema	Incorrecto	6
Seguridad operacional	Actividad de registro de seguridad	Supresión de registro de seguridad	Correcto	6
Seguridad operacional	Actividad de registro de seguridad	Supresión de registro de seguridad	Incorrecto	6

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Acceso al sistema	Actividad de autenticación	Retroceso de autenticación	Incorrecto	6
Acceso al sistema	Actividad de autenticación	Inicio de autenticación	Incorrecto	6

Creación de una consulta para recuperar sólo eventos graves

Puede crear una consulta desde el principio si no encuentra una consulta predefinida que recupere los tipos de eventos de los que desee recibir una notificación. Observe los tipos siguientes de eventos graves:

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Seguridad de host	Actividad del antivirus	Cuarentena de virus	Incorrecto	6
Seguridad de host	Actividad de IDS/IPS	Infracción de firmas	Correcto	6
Seguridad de red	Actividad de infracción de firmas	Infracción de firmas	Correcto	6

Ejemplo: Creación de una consulta para recuperar sólo errores de cuarentena de virus

Por ejemplo, suponga que desea que se le informe de los errores de cuarentena de los virus. Es posible que la palabra cuarentena no aparezca en la lista de consultas. Si es así, puede crear la consulta que necesite y, a continuación, programar una alerta que ejecute esa consulta.

Para crear una consulta que recupere los errores de cuarentena de los virus

1. Haga clic en Consultas e informes.
2. En las opciones de la lista de consultas, seleccione Nuevo.
Aparecerá el asistente de diseño de consulta y mostrará el paso de detalles.
3. Introduzca un nombre.
Por ejemplo, introduzca Alerta: error de cuarentena de virus
4. Introduzca una etiqueta personalizada.
Por ejemplo, Cuarentena de virus.
5. Haga clic en el paso Columnas de consulta y agregue las columnas que desee.
6. Haga clic en el paso de filtros de consulta.
7. Introduzca un filtro simple basado en la entrada de gramática de eventos comunes para el evento.

Por ejemplo, seleccione Seguridad del host para la categoría, Actividad de antivirus para la clase, Cuarentena de virus para la acción y F para el resultado.

Filtros simples	
Seleccione y disponga los filtros simples válidos	
☐ El modelo ideal es	
☒ La categoría del evento es	Host Security
☒ La clase del evento es	Antivirus Activity
☒ La acción del evento es	Virus Quarantine
☐ El nombre del registro de eventos es	
☒ El resultado del evento es	F

8. Seleccione el paso Condiciones de resultado y elija Últimos 5 minutos en la lista desplegable Intervalos predefinidos para asegurarse de que la alerta se genere a tiempo.
9. Haga clic en Guardar y cerrar.

Personalización de consultas para recuperar sólo eventos graves

Las consultas predefinidas que no están etiquetadas como alertas de acción están diseñadas para informes. Es adecuado que los informes contengan datos que reflejen todos los niveles de severidad. Puede personalizar las consultas seleccionadas para sólo recuperen eventos graves. Para ello, identifique una consulta que recupere eventos graves junto con eventos menos graves, cópiela, introduzca filtros que le garanticen que sólo se recuperen los eventos graves y guárdela para seleccionarla en una alerta.

Antes de empezar, tenga a mano una hoja de cálculo que muestre las definiciones de los eventos graves. Este ejemplo se basa en la siguiente información de la gramática de eventos comunes:

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Seguridad operacional	Actividad del sistema	Cierre del sistema	Correcto	7
Seguridad operacional	Actividad del sistema	Cierre del sistema	Incorrecto	7

La consulta que se va a personalizar recupera eventos para inicio y cierre del sistema.

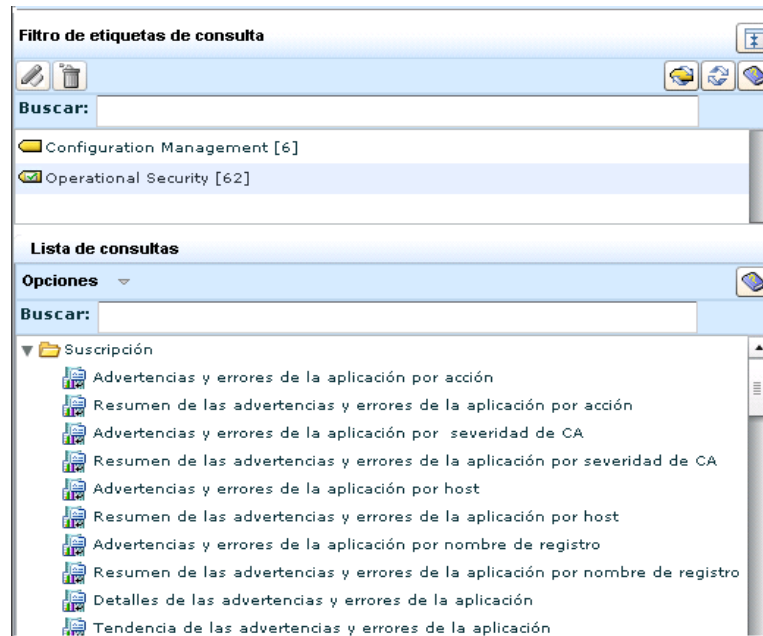
Para personalizar una consulta con el fin de recuperar sólo los eventos graves

1. Haga clic en la ficha Consultas e informes.
2. Seleccione un filtro de etiqueta de consulta que coincida con la categoría de un evento grave.

Por ejemplo, seleccione Seguridad operativa.

3. Revise la lista de consultas con nombres que contengan las palabras clave encontradas en la clase o la acción para el tipo de evento identificado.

Por ejemplo, las palabras clave Cierre del sistema aparecerán en las consultas que comiencen con la frase Inicio o cierre del sistema por host.



4. Copia la consulta Detalles del inicio o cierre del sistema por host. Resalte la consulta y seleccione Copiar en la lista desplegable Opciones.
5. Haga clic en Filtros de consulta y compare los valores predeterminados con las entradas de la tabla para el tipo de evento grave.

En esta consulta está seleccionado Seguridad operativa.

6. Consulte la tabla para conocer los valores que se deben introducir para clase y acción.

Por ejemplo, seleccione Actividad del sistema para la clase y Cierre del sistema para la acción.

Filtros simples

Seleccione y disponga los filtros simples válidos

☐	El modelo ideal es	
☒	La categoría del evento es	Operational Security
☒	La clase del evento es	System Activity
☒	La acción del evento es	System Shutdown
☐	El nombre del registro de eventos es	
☐	El resultado del evento es	

7. Seleccione la ficha Filtros avanzados para determinar si es necesario realizar una modificación.

Haga clic en Suprimir en cada línea dado que el filtro event_action es igual a inicio o cierre del sistema no es pertinente para esta consulta personalizada.

8. Sustitúyalo por un filtro para el resultado.

Por ejemplo, cree un filtro en el que event_result sea igual para correcto o incorrecto.

Filtros avanzados

Para filtrar los eventos, defina una sentencia condicional en el control de filtros.

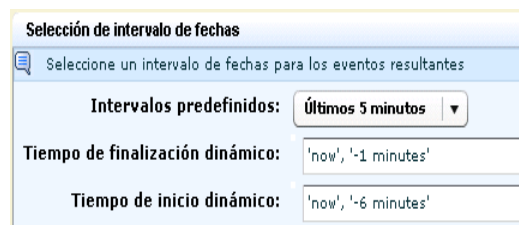
Lógica	(	Columna	Función	Operador	Valor
		event_result		Igual a	S
Or		event_result		Igual a	F

9. Haga clic en Detalles y asigne un nombre de la consulta de manera que indique que desea utilizarla para una alerta.

Por ejemplo, introduzca Alerta: detalle de cierre del sistema por host como nombre. Cambie la descripción en consecuencia.

10. Haga clic en Condiciones de resultado. Para las condiciones graves, considere la posibilidad de utilizar consultas con frecuencia.

Por ejemplo, seleccione el intervalo predefinido para los últimos cinco minutos para ejecutar la consulta cada cinco minutos para la aparición de este evento grave.



Selección de intervalo de fechas

Seleccione un intervalo de fechas para los eventos resultantes

Intervalos predefinidos: Últimos 5 minutos ▼

Tiempo de finalización dinámico: 'now', '-1 minutes'

Tiempo de inicio dinámico: 'now', '-6 minutes'

11. Haga clic en Guardar.

Puede crear una alerta con esta consulta para notificar a una persona, un producto o un proceso si el intento de cierre del sistema ha sido correcto o incorrecto. (La notificación del producto se lleva a cabo a través de traps de SNMP; la notificación del proceso se lleva a cabo a través de salida de alerta/evento de IT PAM.)

Consultas idóneas para modificación

Observe la modificación de las consultas predefinidas seleccionadas para utilizarlas con alertas. Para personalizar la consulta, agregue el filtro simple basado en el análisis de la gramática de eventos comunes. Configure la selección de intervalo de fechas con el intervalo predefinido, Últimos 5 minutos, para asegurarse de que la notificación sea inmediata. A continuación, se muestran algunos ejemplos:

Consulta de error de configuración correcta

1. Copie Detalles de la actividad de error de configuración.

Esta consulta devuelve tanto los resultados correctos como los incorrectos. Sólo se necesitan los resultados correctos.

2. Configure el filtro simple como se indica a continuación:

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Gestión de configuraciones	Gestión de configuraciones	Error de configuración	Correcto	6

3. Guarde como alerta: error de configuración correcto

Consulta para creación de archivo de control correcta

1. Copie Detalles de la actividad de manipulación de datos

Esta consulta recupera todas las acciones de acceso a los datos.

2. Configure el filtro simple como se indica a continuación:

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Acceso a datos	Gestión de objetos	Creación de archivo de control	Correcto	6

3. Guarde como alerta: creación de archivo de control correcta

Consulta para error de exploración antivirus

1. Copie Actividad de virus por acción

Esta consulta filtra todas las acciones de seguridad de host antivirus.

- Utilice la definición siguiente como guía:

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Seguridad de host	Actividad del antivirus	Error de análisis	Correcto	6

- Defina el filtro simple como se indica a continuación:

Copy of Virus Activity by Action

Filtros simples

Filtros avanzados

Filtros simples


 Seleccione y disponga los filtros simples válidos

☒ El modelo ideal es

Antivirus

☒ La categoría del evento es

Host Security

☒ La clase del evento es

Antivirus Activity

☒ La acción del evento es

Virus Scan

☐ El nombre del registro de eventos es

☒ El resultado del evento es

F

- Guarde como alerta: error de exploración de virus

Consulta para error de limpieza de virus

Puede utilizar la consulta predefinida Detección de virus o Detalle de la actividad de detección para recuperar ambas acciones, tanto con resultados correctos como incorrectos. Esto puede ser suficiente para sus necesidades. Opcionalmente puede crear dos consultas separadas basadas en esta consulta en las que especifique el resultado tal como se indica en la tabla de gramática de eventos comunes para eventos graves.

1. Copie Detección de virus o Detalle de la actividad de detección.
2. Cree un filtro simple para especificar el resultado incorrecto.

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Seguridad de host	Actividad del antivirus	Eliminación de virus	Incorrecto	6

3. Elimine el filtro avanzado.
4. Guarde como alerta: error de limpieza de virus

Consulta para detección correcta de un virus

Puede utilizar la consulta predefinida Detección de virus o Detalle de la actividad de detección para recuperar ambas acciones, tanto con resultados correctos como incorrectos. Esto puede ser suficiente para sus necesidades. Opcionalmente puede crear dos consultas separadas basadas en esta consulta en las que especifique el resultado tal como se indica en la tabla de gramática de eventos comunes para eventos graves.

1. Copie Detección de virus o Detalle de la actividad de detección.
2. Cree un filtro simple para especificar el resultado correcto sólo con la actividad de detección.

Categoría	Clase	Acción	Resultado	Nivel de seguridad
Seguridad de host	Actividad del antivirus	Detección de virus	Correcto	6

3. Elimine el filtro avanzado.
4. Guarde como alerta: virus detectado

Consideraciones de las alertas de acción

Puede ver los resultados de cualquier alerta de acción de CA Enterprise Log Manager sin ninguna configuración especial. Además, una alerta de acción se puede enviar a los siguientes destinos:

- Fuente RSS
- Destinatarios de correo electrónico
- Destinos de mensajes SNMP como, por ejemplo, CA Spectrum o CA NSM
- Un proceso de salida de alerta/evento de CA IT PAM

Los administradores configuran estos destinos en la ficha Administración, en Configuración global o Configuración del servicio global: servidor de informes.

Asegúrese de que estos destinos estén configurados como se indica a continuación antes de intentar programar una alerta.

- Para emplear el lector de fuentes, asegúrese de no seleccionar la casilla de verificación La visualización de las alertas de acción requiere autenticación en la configuración global.

A continuación, se muestra la URL de fuente RSS, donde *elmhostname* es el nombre del host del servidor de CA Enterprise Log Manager:

```
https://{elmhostname}:5250/spin/cal/getActionQueryRssFeeds.csp
```

- Para enviar alertas a los destinatarios de correo electrónico, asegúrese de que la sección Configuración del correo electrónico en Configuración del servicio global: servidor de informes.
- (Opcional) Para enviar alertas a los destinos de SNMP, asegúrese de que la sección Configuración de SNMP esté configurada en Configuración del servicio global: servidor de informes.
- Para enviar alertas al proceso de salida de alerta/evento de CA IT PAM, asegúrese de que la sección IT PAM esté configurada en Configuración del servicio global: servidor de informes. (El único valor que no es necesario para las alertas es el del proceso de valores dinámicos.)

Al especificar las condiciones de resultado para una alerta de acción, tenga en cuenta lo siguiente:

- Utilice la hora de inicio y la hora de finalización dinámicas predeterminadas para los intervalos predefinidos.
 - El intervalo predefinido, últimos 5 minutos, está establecido con la hora de finalización dinámica como 'ahora', '-2 minutos' y la hora de inicio dinámica como 'ahora', '-7 minutos'. Este intervalo predeterminado y los otros intervalos de tiempo predefinidos permitirán disponer del tiempo adecuado para guardar los eventos en la base de datos.
- Nota:** No cambie la hora de finalización dinámica a '*ahora*' ni a '*ahora*', '-1 minuto'. Este cambio del valor predefinido puede hacer que se muestren datos incompletos al ejecutar la URL desde el destino. Por ejemplo, si el recuento de eventos es uno de los valores, el recuento que aparece al visualizarlo desde la URL puede ser inferior al recuento que aparece al hacerlo desde CA Enterprise Log Manager.
- Amplíe la hora de finalización dinámica si aparecen datos incompletos con la configuración predeterminada. Por ejemplo, establézcala en 'ahora', '-10 minutos'.

Al crear una programación de alertas de acción, tenga en cuenta lo siguiente:

- El intervalo de repetición es la frecuencia con la que se ejecuta la consulta. Por lo tanto, un intervalo de repetición de 5 minutos indica que la consulta se ejecuta cada cinco minutos o 12 veces cada hora. Las alertas de acción sólo se generan si la consulta devuelve resultados mientras se está ejecutando.
- Establezca el intervalo de repetición según la importancia que tenga para usted la rapidez a la hora de reaccionar cuando se produzca la condición comprobada.
 - Si necesita actuar inmediatamente para tratar la condición, establezca el intervalo de repetición en una frecuencia alta, de manera que la notificación se realice lo antes posible.
 - Si desea realizar un seguimiento de la condición, pero no es necesario intervenir, establezca el intervalo de repetición a una frecuencia baja.
- Intente no establecer el intervalo de repetición en una frecuencia elevada, como cada cinco minutos, si la hora del servidor de CA Enterprise Log Manager no está sincronizada con el servidor de NTP.

Importante: La hora de su servidor de CA Enterprise Log Manager debe estar sincronizada con su servidor de NTP para asegurarse de que se devuelven resultados completos cuando la consulta está configurada para que se ejecute con una frecuencia elevada.

Tenga en cuenta las siguientes opciones de filtrado:

- Para usar los filtros que se definen con las consultas incluidas, no se necesita ninguna acción.
- Para aplicar filtros adicionales para las consultas incluidas en una alerta, defínalas en el paso Filtros de alerta.
- Para aplicar el mismo conjunto de filtros a varias tareas de alerta, utilice un perfil.

Antes de configurar umbrales para alertas de acción en un servidor de informes de CA Enterprise Log Manager, tenga en cuenta lo siguiente:

- Para mantener un tamaño razonable de la fuente RSS, defina el número máximo de alertas que se permitirán. Cuanto más frecuentes sean los intervalos de repetición de las alertas activadas, más rápidamente se llenará la fuente con los resultados obtenidos por las consultas.
- Para asegurarse de que la fuente RSS no retiene alertas durante más tiempo que el que le interesa, establezca la retención de alertas de acción a un valor equivalente a la antigüedad máxima de días del registro más antiguo que va a retener.
- Tenga en cuenta la frecuencia con la que desea comprobar la fuente RSS para revisar las alertas. Esta frecuencia puede ayudarle a planificar el tiempo durante el que desea guardar los registros.
- Si desea que la fuente RSS muestre los resultados más recientes de todas las tareas en todo momento, configure los valores de retención de manera que las alertas de ejecuciones poco frecuentes no se eliminen por ser más antiguas que las alertas de ejecuciones frecuentes que llenan la capacidad de la cola.

Más información:

[Configuración de retenciones de alertas de acción](#) (en la página 496)

[Ejemplo: Crear una alerta de acción para el espacio en disco bajo](#) (en la página 486)

Trabajo con procesos de salida de alerta/evento de CA IT PAM

Para trabajar con procesos de salida de alerta/evento de CA IT PAM que están integrados en CA Enterprise Log Manager es necesario combinar algunas de las tareas siguientes:

- Importar el ejemplo del proceso de salida de alerta/evento
- Crear procesos de salida de alerta/evento que cumplan los requisitos de integración de CA IT PAM.
- Configurar la integración de CA IT PAM y especificar el proceso de salida de alerta/evento predeterminado
- Ejecutar procesos de salida alerta/evento a partir de los resultados de la consulta seleccionada
- Programar alertas que ejecuten un proceso de CA IT PAM por fila
- Programar alertas que ejecuten un proceso de CA IT PAM por consulta

Más información:

[Importación del proceso de salida de alerta/evento de ejemplo](#) (en la página 400)

[Directrices para la creación de un proceso de alerta/evento](#) (en la página 407)

[Ejemplo: Ejecución de un proceso de salida de alerta/evento con resultados de la consulta seleccionada](#) (en la página 415)

[Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por fila](#) (en la página 421)

[Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por consulta](#) (en la página 426)

Acerca de los procesos de salida de alerta/evento de CA IT PAM

CA Enterprise Log Manager detecta eventos que requieren intervención. Es posible generar alertas en cuanto se producen los eventos no deseados. La integración con CA IT PAM permite que una alerta ejecute un proceso de salida de alerta/evento. Los procesos de alerta/evento están diseñados para invocar medidas apropiadas para la solución del problema mediante otros productos. Es decir, los procesos de salida de alerta/evento son procesos de CA IT PAM que ordenan a otros productos que tomen medidas concretas sobre los objetos especificados.

CA Enterprise Log Manager, CA IT PAM y otros productos de terceros trabajan conjuntamente para proteger su entorno. CA Enterprise Log Manager automatiza la detección de eventos no deseados y el proceso de salida de alerta/evento de IT PAM invoca otros productos para que lleven a cabo la serie de respuestas adecuada.

La integración implica la configuración de la conexión con el servidor de CA IT PAM, mediante la especificación del proceso que se ejecutará y de los parámetros del proceso con valores predeterminados.

La ejecución del proceso de CA IT PAM se puede realizar a petición a partir de los resultados (fila) de la consulta que se muestran o a través de alertas programadas. En ambos casos, los valores de los parámetros, como el resumen y la descripción, se pueden personalizar para proporcionar detalles útiles para el producto de destino del proceso de CA IT PAM.

Más información:

[Arquitectura que admite la integración de CA IT PAM](#) (en la página 393)

[Proceso de trabajo con procesos de salida de alerta/evento](#) (en la página 393)

[Cómo funciona la integración de CA IT PAM](#) (en la página 395)

[Ejemplo: Flujo de datos para procesamiento de alerta/evento](#) (en la página 398)

Arquitectura que admite la integración de CA IT PAM

Para ejecutar un proceso de salida de alerta/evento de CA IT PAM, necesita los siguientes componentes de red:

- Un entorno de trabajo de CA Enterprise Log Manager, por ejemplo:
 - Agentes con conectores que capturen eventos sin procesar de orígenes de eventos.
 - Servidores de recopilación de CA Enterprise Log Manager que refinan los eventos sin procesar y los envíen a los servidores de informes.
 - Servidores de informes de CA Enterprise Log Manager que procesen las alertas programadas y las consultas a petición.
- Un servidor de CA IT Process Automation Manager r2.1 (CA IT PAM) configurado con procesos que invoquen otro producto para realizar una acción de solución de problemas rutinaria.
- Un servidor con un producto utilizado por el proceso de CA IT PAM, por ejemplo, un servidor con un producto de departamento de asistencia técnica.

Proceso de trabajo con procesos de salida de alerta/evento

A continuación se muestra una descripción general del flujo de trabajo para aprovechar un proceso de salida de alerta/evento de CA IT PAM:

1. Determine si va a configurar la integración de CA IT PAM con o sin el ejemplo de proceso. La ventaja de usar el ejemplo de proceso es que permite ver los resultados de inmediato. Puede aplazar la actualización de su propio proceso hasta que se haya familiarizado con los resultados de la integración. El uso de un ejemplo de proceso requiere CA Service Desk.
2. Puede realizar una de las acciones siguientes o ambas:
 - Importar el ejemplo de proceso y especificar los parámetros de conexión de CA ServiceDesk.
 - Crear procesos de salida de alerta/evento que cumplan los requisitos de integración de CA Enterprise Log Manager.
3. Recopile detalles para la integración de CA IT PAM a partir de ejemplo de proceso o del proceso que haya creado.
4. Configure la integración de CA IT PAM para salida de alerta/evento

5. Asegúrese de que los usuarios que controlen los resultados del proceso de salida de alerta/evento en el producto de terceros tengan cuentas de usuario en CA Enterprise Log Manager y conozca las credenciales con las que vaya a iniciar sesión. Puede asignar la función de Auditor a estas cuentas.

Nota: Cuando los usuarios inician sesión, lo único que pueden hacer es ver la página con los resultados de la consulta asociada.

6. Prepárese para automatizar la ejecución de un proceso de salida de alerta/evento:
 - a. Identifique la consulta o las consultas que devuelvan datos sobre los que el producto de terceros pueda tomar medidas de acuerdo con el proceso de CA IT PAM configurado.
 - b. Si la consulta utiliza una lista con clave, asegúrese de que esta lista contenga los valores que necesite.
 - c. Ejecute el proceso de salida de alerta/evento sobre los resultados de la consulta y verifique que el proceso se ejecute correctamente.
7. Programe un alerta de acción mediante el procedimiento documentado y siga las directrices que se indican a continuación.
 - a. En el paso Selección de alertas:
 - Introduzca un nombre de tarea.
 - Verifique si el tipo de selección es Consultas.
 - Seleccione una o varias consultas que haya identificado durante la planificación.
 - b. En el paso Destino, seleccione la ficha Proceso de IT PAM y especifique detalles de salida de alerta/evento, como se indica a continuación:
 - Seleccione las consultas en las que vaya a basar la alerta.
 - Determine si se ejecutará el proceso una vez por cada consulta que devuelva resultados o una vez por cada fila devuelta.
 - Especifique los valores de los parámetros del proceso de IT PAM. Sólo puede incluir valores de campo y texto para los valores de los parámetros Resumen y Descripción si el proceso se ejecuta por fila.
 - c. Especifique detalles para el resto de los pasos al igual que con todas las alertas de acción que programa y, a continuación, guárdelos y cierre el asistente.

8. Controle los resultados:
 - a. Verifique si la lista Tareas de alerta de acción incluye esta tarea.
 - b. Controle los eventos autocontrolados y la acción de notificación de eventos para verificar que el resultado de la ejecución del proceso de IT PAM es correcto.
 - c. (Opcional) Inicie sesión en el producto de terceros que haya respondido a la información de salida de alerta/evento de CA Enterprise Log Manager que se haya enviado mediante el proceso de IT PAM.

Más información:

[Importación del proceso de salida de alerta/evento de ejemplo](#) (en la página 400)

[Directrices para la creación de un proceso de alerta/evento](#) (en la página 407)

[Ejemplo: Ejecución de un proceso de salida de alerta/evento con resultados de la consulta seleccionada](#) (en la página 415)

[Diseño de consultas para eventos que se envían al proceso de salida de alerta/evento](#) (en la página 419)

[Configuración de destinos de las notificaciones](#) (en la página 479)

[Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por fila](#) (en la página 421)

Cómo funciona la integración de CA IT PAM

Supongamos que se ha realizado la siguiente configuración:

- Ha configurado CA IT PAM en la página de configuración del servidor de informes y ha especificado el proceso de salida de alerta/evento que se ejecutará.
- Ha programado una alerta con CA IT PAM como destino y ha especificado que el proceso se ejecute una vez por fila. Para los parámetros que permiten la entrada de instrucciones de resumen y descripción, ha introducido instrucciones que incluyan campos de la gramática de eventos comunes.
- Ha programado otra alerta con CA IT PAM como destino y ha especificado que el proceso se ejecute una vez por consulta. Para los parámetros que permiten la entrada de instrucciones de resumen y descripción, ha introducido texto literal.

El proceso completo incluye acciones de varios orígenes:

- La generación de eventos sin formato mediante orígenes de eventos
- La recopilación y el refinamiento de eventos mediante CA Enterprise Log Manager
- La generación de alertas cuando los eventos refinados cumplen los criterios de consulta de eventos mediante CA Enterprise Log Manager
- El envío de una salida de alerta y evento mediante CA Enterprise Log Manager a CA IT PAM
- La ejecución del proceso de salida de alerta/evento mediante CA IT PAM en un sistema de terceros
- Uno de los siguientes:
 - Una evaluación de los datos por parte de usuario del sistema de terceros quien determina la acción correcta y la lleva a cabo.
 - La respuesta automática mediante el sistema de terceros para los eventos que se produzcan.

A continuación, presentamos un resumen del proceso:

1. Los orígenes generan eventos sin formato.
2. Los agentes recopilan algunos de estos eventos sin formato basados en sus conectores y transfieren los eventos sin formato a un servidor de recopilación.
3. Este servidor normaliza y clasifica los eventos sin formato y transfiere los eventos refinados a un servidor de informes.

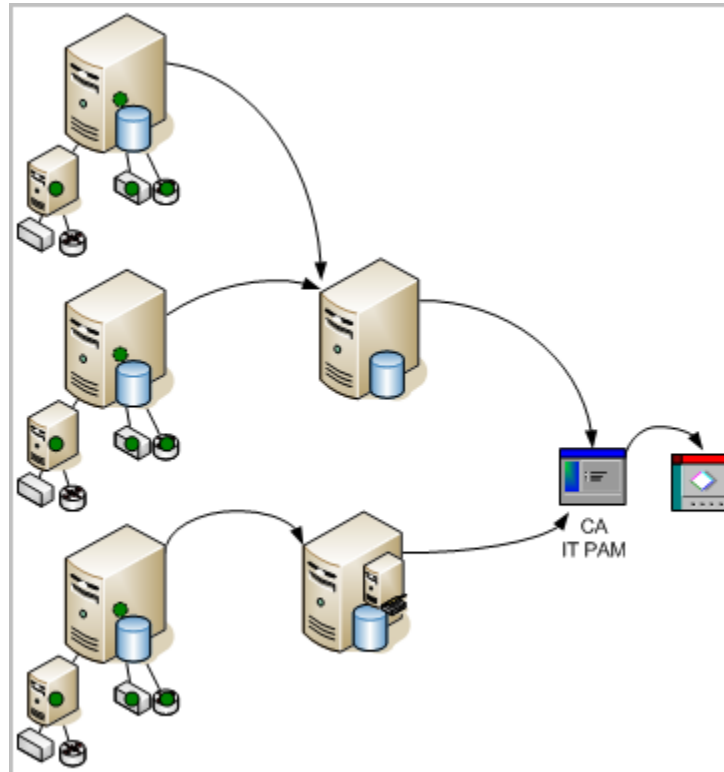
Por ejemplo, cuando se realiza un cambio de configuración en un sistema, se crea un registro y se clasifica como un cambio de configuración. El evento captura la hora del cambio, el host en el que se ha realizado, el usuario que lo ha llevado a cabo y el resultado del intento de cambio.
4. El servidor de informes ejecuta las consultas seleccionadas para cada alerta programada.

5. Si los eventos refinados cumplen los criterios de la consulta, el servidor de informes genera una alerta y transfiere la siguiente información a CA IT PAM:
 - Detalles de la alerta
 - Muestra los parámetros y los valores del proceso.
 - Los campos de la gramática de eventos comunes se envían para los parámetros del proceso no mostrados.
 - Detalles del evento
 - Para cada fila, los detalles del evento se transmiten mediante las entradas de los campos disponibles para las instrucciones de resumen y descripción, en las que los usuarios describen el evento con las variables de los campos de la gramática de eventos que forman la consulta seleccionada para la alerta.
 - Para cada consulta, los detalles del evento se transmiten con una dirección URL a una página de CA Enterprise Log Manager que muestra detalles del evento en el nivel de fila.
6. Si el envío es correcto, CA IT PAM continúa con el procesamiento, de acuerdo con lo definido en el proceso de salida de alerta/evento configurado.
7. Si el producto de terceros es CA Service Desk y el proceso es el ejemplo del proceso de salida de alerta/evento, ocurrirá lo siguiente:
 - Se abrirá un parte del departamento de asistencia técnica y se le asignará un número. Los campos del parte se rellenarán con los valores de los parámetros de la definición de la alerta. Si se recibe una dirección URL, se mostrará con la instrucción de resumen.
 - CA Service Desk devolverá el número del parte a CA IT PAM.
8. CA IT PAM devolverá el número del parte a CA Enterprise Log Manager.
9. CA Enterprise Log Manager mostrará el número del parte como un evento autocontrolado.

Ejemplo: Flujo de datos para procesamiento de alerta/evento

En el diagrama siguiente, las flechas muestran el flujo de datos:

- De servidores de recopilación a servidores de informes
- De servidores de informes a CA IT PAM
- De CA IT PAM al producto al que el proceso de CA IT PAM envía la salida de CA Enterprise Log Manager, por ejemplo, CA Service Desk.

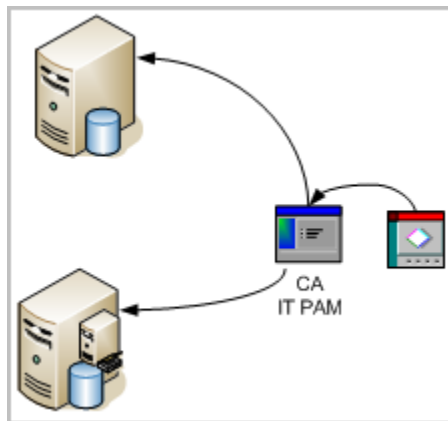


Cuando se notifique a CA Enterprise Log Manager que el envío ha sido correcto, sondeará CA IT PAM para conocer el estado del proceso que se haya ejecutado. En cuanto CA IT PAM envíe la actualización del estado, CA Enterprise Log Manager creará un evento autocontrolado con el resultado. La secuencia de procesamiento es la siguiente:

1. CA IT PAM notifica a CA Enterprise Log Manager si el proceso se ha ejecutado correctamente o no.
2. CA Enterprise Log Manager genera un evento autocontrolado de creación de notificación con el resultado recibido.

Observe el ejemplo en el que el proceso de CA IT PAM crea un parte del departamento de asistencia técnica con valores de los parámetros del proceso y los datos del evento recuperados mediante la consulta. En el diagrama siguiente, las flechas muestran el flujo de datos siguiente:

- Desde el producto del departamento de asistencia técnica a CA IT PAM
- Desde CA IT PAM a los servidores de informes de CA Enterprise Log Manager de origen



Importación del proceso de salida de alerta/evento de ejemplo

Para que pueda probar la integración de CA IT PAM de inmediato y poner en práctica el procedimiento de configuración con valores conocidos, CA proporciona un ejemplo de proceso con este fin. Se encuentra en el DVD de la aplicación. En este ejemplo del proceso de IT PAM se supone que utiliza CA Service Desk como su aplicación de departamento de asistencia técnica.

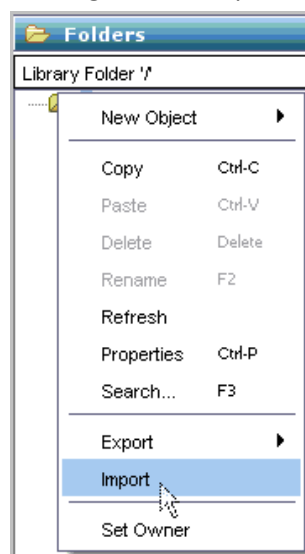
A continuación, configure CA IT PAM en CA Enterprise Log Manager y pruebe la ejecución de este ejemplo del proceso de CA IT PAM con los resultados de la consulta que seleccione. Cuando esté familiarizado con el funcionamiento de CA Enterprise Log Manager con CA IT PAM, podrá asegurarse de la conformidad de su propio proceso y sustituir estos valores en la configuración de CA IT PAM por su integración de productos.

Para importar un ejemplo de proceso y probar la integración de IT PAM

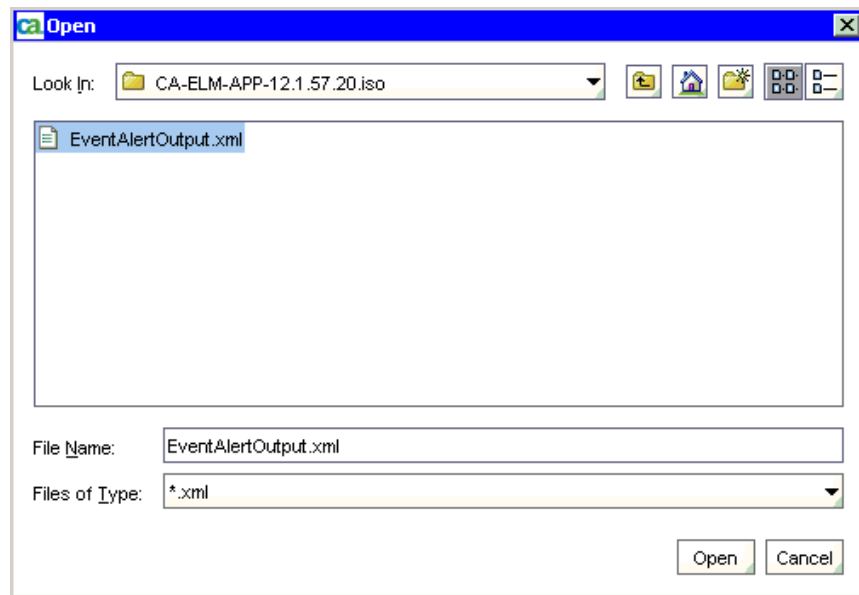
1. Inicie CA IT PAM e inicie sesión.
2. Inicie el cliente de ITPAM.



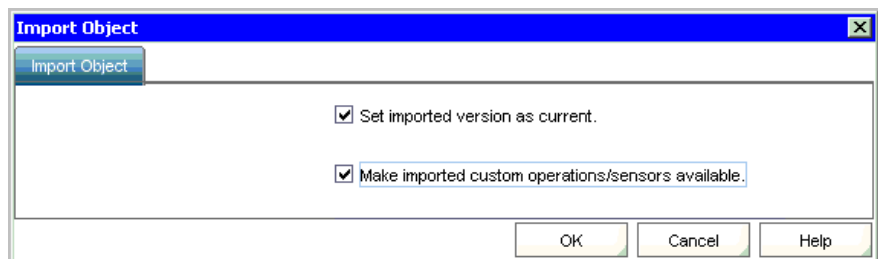
3. Importe el ejemplo de proceso de IT PAM, EventAlertOutput.xml, que se incluye en el DVD de la aplicación, dentro de CA/ITPAM. Este ejemplo tiene todos los valores necesarios que se han definido.
 - a. Seleccione Archivo, Abrir explorador de bibliotecas.
 - b. En el panel de la izquierda, haga clic en Carpetas y en la carpeta raíz, haga clic en Importar.



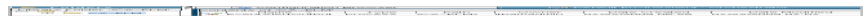
- c. Seleccione el ejemplo de proceso de IT PAM, EventAlertOutput.xml, de la imagen iso extraída y haga clic en Abrir.



- d. Seleccione ambas opciones en el cuadro de diálogo Importar objeto y haga clic en Aceptar.



Como resultado, se mostrará el nombre y la ruta exactos. Por ejemplo, el nombre es EventAlertOutput y la ruta es /CA_ELM/.



4. Especifique los parámetros de conexión del centro de servicio al usuario.
- Haga clic en la ficha Parámetros de conexión al centro de servicio al usuario para Request_Create con el fin de ver los parámetros de conexión al centro de servicio al usuario.
 - Utilice la siguiente sintaxis para especificar la URL del centro de servicio al usuario:

```
"http://<server name>:8080/axis/services/USD_R11_WebService"
```
 - Introduzca las credenciales válidas de inicio de sesión de ID de usuario y contraseña del centro de servicio al usuario.

5. (Opcional) Pruebe el proceso importado para asegurarse de que funciona como un proceso independiente.
6. Cierre el cliente de ITPAM y, a continuación, haga clic en Cerrar sesión para salir de CA IT PAM.

Visualización del ejemplo de proceso de salida de alerta/evento

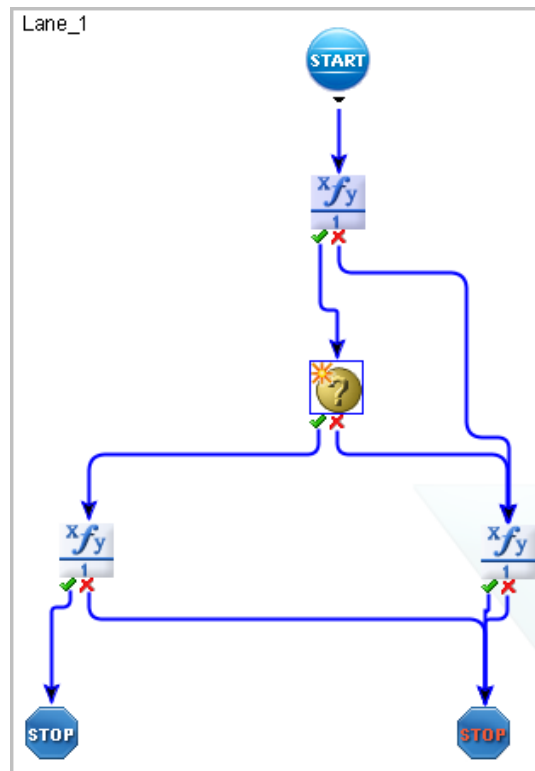
Si se importa el ejemplo de proceso de salida de alerta/evento, se puede examinar su diseño en CA IT PAM. Utilice las directrices siguientes para familiarizarse con los requisitos de CA Enterprise Log Manager en el contexto del ejemplo de proceso. A lo largo de esta descripción, podrá ver dónde se definen los parámetros de conexión del servicio Web y cómo se definen los operadores de cálculo. Además, observará los requisitos específicos del producto. Por ejemplo, para configurar CA Service Desk como el producto de terceros, es necesario utilizar el operador Request_Create desde el módulo CA Service Desk y un operador de cálculo previo que mantenga los valores de severidad y prioridad.

Para familiarizarse con el ejemplo del proceso de salida de alerta/evento

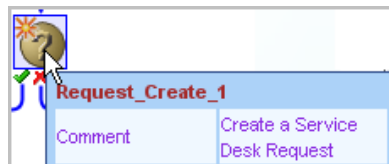
1. Muestre el modelo de su proceso de destino.
 - a. Inicie CA IT PAM e inicie sesión.
 - b. Haga clic en el cliente de ITPAM.
 - c. En el menú Archivo, seleccione Abrir explorador de bibliotecas.
 - d. En la ficha Carpetas, seleccione la carpeta de bibliotecas que contenga el modelo para su proceso de destino.

El nombre del proceso y la ruta aparecerán en el panel principal.
 - e. Haga doble clic en la fila que contenga el nombre y la ruta del proceso.

Aparecerá un modelo parecido al siguiente: Este ejemplo de modelo contiene los requisitos mínimos para CA Enterprise Log Manager.



2. Observe cómo cumplen los parámetros básicos de ServiceDesk los requisitos de CA Enterprise Log Manager.
 - a. Haga doble clic en el icono Request_Create_1.



El operador Request_Create enviará los datos devueltos por la consulta de alerta de acción al producto de destino (aplicación). Se necesita un operador parecido para cualquier proceso que se vaya a ejecutar desde CA Enterprise Log Manager.

- b. En Parámetros básicos de ServiceDesk, observe que los parámetros locales del proceso se especifican con la sintaxis siguiente:

BasicParameter = Process.LocalParameter

Nota: Los parámetros locales del proceso son los parámetros del proceso de salida de alerta/evento que se agregan a CA Enterprise Log Manager cuando se configura CA IT PAM.

Parámetros del proceso de salida de alerta/evento
ReportedBy
Summary
Description
EndUser
Priority
Severity

- c. Dado que la aplicación de destino es el producto CA Service Desk, los siguientes parámetros locales del proceso se definen tal y como se describe en la tabla siguiente:

Parámetro básico de ServiceDesk	Parámetro local	Campo de Service Desk	Notas
ID del creador de la solicitud	Process.ReportedBy	Asignatario, Comunicado por	Un "contacto" válido de CA Service Desk
Resumen	Process.Summary	Resumen	(Dejar en blanco)
Descripción	Process.Description	Descripción	(Dejar en blanco)
ID de cliente	Process.EndUser	Usuario final afectado	Un "contacto" válido de CA Service Desk
Prioridad	Process.Priority	Prioridad	1-5
Gravedad	Process.Severity	Gravedad	1-5

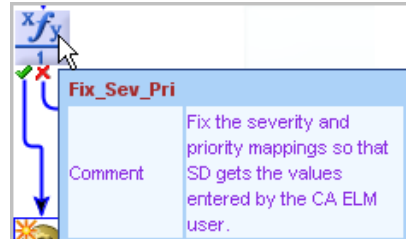
En el ejemplo siguiente se muestran los parámetros locales válidos para los parámetros básicos de ServiceDesk. Las entradas distinguen entre mayúsculas y minúsculas. Es decir, Process.ReportedBy se debe introducir exactamente como se muestra, por ejemplo, con una "R" mayúscula y una "B" mayúscula.

The screenshot shows a window titled 'Properties of Request_Create_1'. Inside, there is a tab labeled 'ServiceDesk Basic Parameters'. The tab contains the following fields:

- *Request Creator ID:
- *Summary:
- *Description:
- *Customer ID:
- *Request Type: (dropdown arrow)
- *Priority: (dropdown arrow)
- *Severity: (dropdown arrow)
- *Impact: (dropdown arrow)
- *Urgency: (dropdown arrow)

3. Haga clic en la ficha Parámetros de conexión al centro de servicio al usuario para Request_Create con el fin de ver los parámetros de conexión al centro de servicio al usuario.
 - URL de Service Desk: "http://<nombre servidor>:8080/axis/services/USD_R11_WebService"
 - ID de usuario de Service Desk: "<usuario SD>"
 - Contraseña: "<contraseña SD>"

4. Observe que para CA Service Desk, se necesita un ajuste para garantizar que los valores de severidad y prioridad que se introduzcan en CA Enterprise Log Manager se interpretan correctamente mediante CA Service Desk.
 - a. Aparece un operador de cálculo previo después de Start y antes del operador Create_Process. En el ejemplo siguiente, se denomina Fix_Sev_Pri.



- b. En Propiedades, Calcular, se definen las siguientes asignaciones:

```
if (Process.Priority == 1) Process.Priority = "pri:504";
else if (Process.Priority == 2) Process.Priority = "pri:503";
else if (Process.Priority == 3) Process.Priority = "pri:502";
else if (Process.Priority == 4) Process.Priority = "pri:501";
else if (Process.Priority == 5) Process.Priority = "pri:500";

if (Process.Severity == 1) Process.Severity = "sev:800";
else if (Process.Severity == 2) Process.Severity = "sev:801";
else if (Process.Severity == 3) Process.Severity = "sev:802";
else if (Process.Severity == 4) Process.Severity = "sev:803";
else if (Process.Severity == 5) Process.Severity = "sev:804";
```
5. Observe que en el siguiente valor devuelto, o interfaz de salida, los parámetros tienen el formato requerido por CA Enterprise Log Manager:
 - ResultString
 - FaultString
6. Observe el operador de cálculo para la creación de solicitud correcta. Este formato se debe utilizar en todos los procesos de salida de alerta/evento que se vayan a ejecutar desde CA Enterprise Log Manager.
 - a. Haga clic en el icono de operador de cálculo para la creación de solicitud correcta.
 - b. Seleccione la ficha Calcular y haga clic en ... en el campo del código de origen.
 - c. Observe cómo se define el operador de cálculo Correcto en el código de origen:

```
Process.ResultString = "Request " + Request_Create_1.newRequestNumber + "
created in CA Service Desk.";
```

7. Observe el operador de cálculo de Error. Este formato es necesario para cualquier proceso de salida de alerta/evento que se vaya a ejecutar desde CA Enterprise Log Manager.
 - a. Haga clic en el icono del operador de cálculo para Error.
 - b. Seleccione la ficha Calcular y haga clic en ... en el campo del código de origen.
 - c. Observe cómo se define el operador de cálculo de Error en el código de origen, en el que Process.FaultString se asigna a la variable de SOAP apropiada:

```
Process.FaultString = Request_Create_1.SoapErrorResponse;
```

Directrices para la creación de un proceso de alerta/evento

Es necesario seguir determinadas pautas para ejecutar un proceso de CA IT PAM desde CA Enterprise Log Manager. Antes de intentar ejecutar un proceso de CA IT PAM desde CA Enterprise Log Manager, compruebe que el proceso incluya:

- Los parámetros de conexión del servicio Web.
- Un operador de cálculo Correcto que asigne Process:ResultString a una instrucción con caracteres literales y variables que exprese la respuesta desde el producto de terceros.
- Un operador de cálculo Error que asigne Process:FaultString a la variable de respuesta de SOAP apropiada.

Si el proceso de IT PAM de destino es para un producto de departamento de asistencia técnica de terceros, compruebe que el proceso también incluya:

- El operador específico del producto.

Por ejemplo, un proceso destinado al BMC Remedy Module se debe definir con el operador Create_Help_Desk_Case.
- Los parámetros específicos del producto que se asignan a parámetros de procesos locales: ReportedBy, Summary, Description, EndUser, Priority y Severity.

Por ejemplo, un proceso destinado al BMC Remedy Module debería asignar parámetros locales a los parámetros de caso de creación del departamento de asistencia técnica.

Por lo general, los procesos de CA IT PAM sólo incluyen los parámetros de procesos predeterminados. Cada uno de éstos está asignado a un campo del producto de terceros. De forma opcional, puede agregar campos de la gramática de eventos comunes como parámetros de procesos para un proceso determinado. En el siguiente ejemplo se muestran los siguientes campos de la gramática de eventos comunes del conjunto de datos:

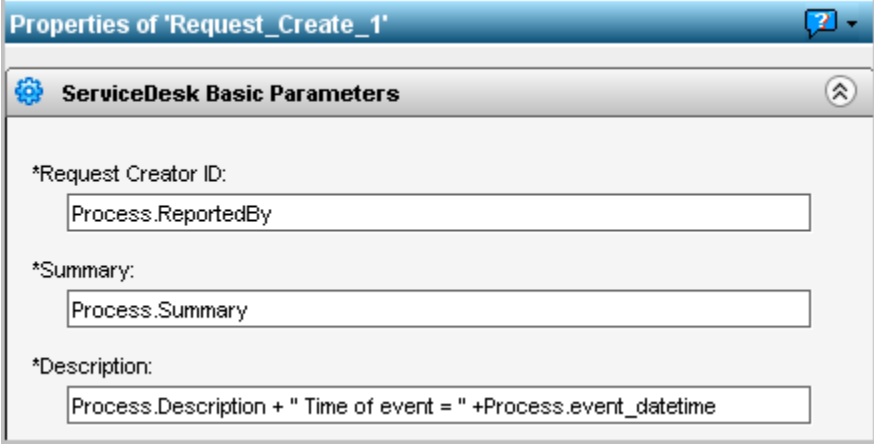
- event_severity
- event_count
- event_datetime

The screenshot shows a configuration window for the 'Dataset' tab. It contains a list of fields with corresponding input boxes:

ReportedBy	
Severity	
Summary	
Description	
Priority	
ResultString	
FaultString	
EndUser	
event_severity	
event_count	
event_datetime	

At the bottom, there are four tabs: 'Main Editor', 'Exception Handler', 'Lane Change Handler', and 'Dataset' (which is currently selected and highlighted in blue).

Cada parámetro básico está asignado a un campo de Service Desk. Por ejemplo, el parámetro de proceso ReportedBy está asignado al campo de CA Service Desk denominado Asignatario. Cuando se agregan campos de la gramática de eventos comunes como parámetros del proceso, se puede hacer referencia a éstos como valores en un parámetro básico. Por ejemplo, puede definirse el valor del campo de la gramática de eventos comunes event_datetime para que aparezca de forma predeterminada en el campo Descripción en CA Service Desk. Esto puede hacerse mediante la adición de Process.event_datetime en el campo Descripción de los parámetros básicos de Service Desk.



The screenshot shows a window titled "Properties of 'Request_Create_1'". Inside, there is a tab labeled "ServiceDesk Basic Parameters". The tab contains three fields with labels and values:

- *Request Creator ID: Process.ReportedBy
- *Summary: Process.Summary
- *Description: Process.Description + " Time of event = " +Process.event_datetime

Al crear una alerta que se ejecute en este proceso, examine los campos de la gramática de eventos comunes que aparecen en Enviar valores del campo como parámetros. Si alguno de los parámetros enumerados es un campo de la gramática de eventos comunes que ha definido como parámetro de proceso, seleccione dicho campo. Observe los siguientes ejemplos:

- Los tres campos de la gramática de eventos comunes definidos en el conjunto de datos se muestran para la consulta Recuento de eventos del sistema por acción de evento. Por lo tanto, debería seleccionar los tres para enviarlos como parámetros a CA IT PAM.

Recuento de eventos del sistema por acción de evento

☒ Ejecutar proceso de CA IT PAM por fila

Proceso de CA IT : /CA_ELM/EventAlertOutput

Seleccionar campo: event_action

ReportedBy: ServiceDesk	+	Enviar valores del campo como parámetros ☒ event_action ☒ event_count ☒ event_datetime
Severity: 4	+	
Priority: 4	+	
EndUser: ServiceDesk	+	
Summary:	+	
Description:	+	

- Dos de los tres campos de la gramática de eventos comunes definidos en el conjunto de datos se muestran para la consulta >5 Inicios de sesión por cuentas de admin. Debería seleccionar dos para enviarlos como parámetros a CA IT PAM.

(>5) Inicios de sesión por cuentas de admin. en sistemas críticos durante la noche para como mínimo 1 día

☒ Ejecutar proceso de CA IT PAM por fila

Proceso de CA IT : /CA_ELM/EventAlertOutput

Seleccionar campo: dest_hostname

ReportedBy: ServiceDesk	+	Enviar valores del campo como parámetros ☐ dest_hostname ☐ dest_username ☒ event_action ☒ event_datetime ☐ event_logname ☐ event_result
Severity: 4	+	
Priority: 4	+	
EndUser: ServiceDesk	+	
Summary:	+	
Description:	+	

Más información:

[Visualización del ejemplo de proceso de salida de alerta/evento](#) (en la página 402)

Obtención de detalles para integración de CA IT PAM

La mayoría de los detalles necesario para la integración de CA IT PAM forman parte de las configuraciones de los productos y los procesos de CA IT PAM. Puede iniciar CA IT PAM y buscar los detalles cuando los necesite para la configuración, o bien puede obtener los detalles en primer lugar, registrarlos y, a continuación, configurar CA IT PAM con rapidez mediante la introducción de los valores registrados.

Puede hacer referencia a los ejemplos de procesos que haya importado o a sus propios procesos que haya modificado para que satisfagan los requisitos de CA Enterprise Log Manager.

Para obtener detalles para integración de CA IT PAM

1. Inicie sesión en su servidor local de CA IT PAM y verifique si es CA IT Process Automation Manager 2.1.
2. Haga clic en el vínculo del cliente de ITPAM.
3. Recopile detalles para los cuatro primeros campos de la configuración de IT PAM.
 - a. Haga clic en el explorador de configuración.
 - b. Haga clic en la ficha Propiedades.
 - c. Registre el valor Nombre de servidor como valor para el servidor de IT PAM.
 - d. Acepte el puerto 8080 como el puerto de IT PAM.
 - e. Obtenga credenciales de inicio de sesión para CA Enterprise Log Manager desde el administrador de CA IT PAM y regístrelas para Nombre de usuario y Contraseña.

Campo de configuración de IT PAM	Descripción	Su valor
Servidor de IT PAM	Nombre de host completo del servidor en el que está instalado CA IT PAM. Este valor aparece en el campo Nombre de servidor Server Name, en la ficha Propiedades del explorador de configuración.	
Puerto IT PAM	El puerto 8080 es el predeterminado. Este valor aparece en la ficha URL de dominio, en la ficha Propiedades del explorador de configuración.	8080
Nombre de usuario	ID de usuario que utilizará CA Enterprise Log Manager para iniciar sesión en IT PAM y ejecutar un proceso. Lo puede obtener de su administrador de CA IT PAM. Ejemplo: itpamadmin	
Contraseña	La contraseña asociada con el nombre de usuario. Lo puede obtener de su administrador de CA IT PAM.	

4. Registre la ruta del proceso y los nombres de los procesos que desee ejecutar desde CA Enterprise Log Manager.
 - a. En el menú Archivo del cliente ITPAM, seleccione Abrir explorador de bibliotecas.
 - b. En la ficha Carpetas, seleccione la carpeta de biblioteca que contenga el proceso de salida de alerta/evento.
 - c. Registre la ruta y el nombre para el proceso de salida de alerta/evento.
 - d. Si es diferente, seleccione la carpeta de biblioteca que contenga el proceso que devuelva valores actuales para una clave especificada.
 - e. Registre el nombre y la ruta para el proceso de valores dinámicos.

Campo específico del proceso de IT PAM	Descripción y ejemplo	Su valor
Proceso de obtención de resultados de eventos/alertas	Nombre de la ruta y el proceso. Identifica el proceso diseñado para enviar detalles configurados con la alerta o una dirección URL a un producto externo, como CA Service Desk. Ejemplo: /CA_ELM/EventAlertOutput	
Proceso de valores dinámicos	Nombre de la ruta y el proceso. Identifica el proceso diseñado para recopilar valores para la clave de entrada y devolverlos para que se analicen en un archivo csv. Ejemplo: /CA_ELM/ValuesList	

5. Recopile parámetros del proceso de salida de alerta/evento:
 - a. Haga doble clic en el proceso Salida de alerta/evento al que hizo referencia para abrir el proceso.
 - b. En la ficha Editor principal, haga clic en el icono Request_Create para mostrar las propiedades.
 - c. Muestre los parámetros básicos de ServiceDesk.
 - d. Registre estos parámetros con el prefijo Process: en la primera columna inferior si no coinciden exactamente con lo que se muestra.
 - e. Haga clic en la ficha Dataset.
 - f. Haga clic en todos los parámetros de Local_Dataset y registre su valor predeterminado, si procede.

Parámetros del proceso de salida de alerta/evento	Descripción y ejemplo	Su valor
ReportedBy	Un nombre de usuario del centro de servicio al usuario válido.	
Resumen	Este texto aparece en el campo Resumen de la solicitud de centro de servicio al usuario. Por ejemplo, "Solicitud creada dese CA ELM"	---
Descripción	Este texto aparece en el campo Descripción de la solicitud de centro de servicio al usuario.	---
Usuario final	Un nombre de usuario del centro de servicio al usuario válido.	
Prioridad	Define la prioridad predeterminada. Si no se configura ningún valor predeterminado, registre un valor comprendido entre 1 y 5. Ejemplo 3:	
Severidad	Define la severidad predeterminada. Si no se configura ningún valor predeterminado, registre un valor comprendido entre 1 y 5. Ejemplo 4:	

Ejemplo: Ejecución de un proceso de salida de alerta/evento con resultados de la consulta seleccionada

Todos los usuarios están autorizados a ejecutar un proceso de CA IT PAM a petición. El proceso de salida de alerta/evento de CA IT PAM configurado se puede ejecutar con resultados de la consulta seleccionada para cualquiera de los fines siguientes:

- Llevar a cabo un proceso de salida de alerta/evento a petición basado en las necesidades actuales.
- Probar los resultados del procesamiento antes de crear una alerta programada para esta consulta con el proceso de CA IT PAM como destino.

El proceso de CA IT PAM se puede ejecutar desde una fila de resultados de la consulta que se muestra. En este caso, se supone que los resultados se muestran como una tabla en lugar de un gráfico. Las filas de resultados de la consulta se pueden mostrar de cualquiera de las maneras que se indican a continuación:

- Seleccione una consulta de la lista de consultas que devuelva resultados.
- Seleccione un informe de la lista de informes y seleccione una consulta que devuelva resultados.
- Introduzca una petición que genere resultados.

Nota: En el tema siguiente se supone que la fila de resultados de la consulta se muestra al seleccionar la consulta en la lista de consultas.

Para familiarizarse con los datos que se devuelven para los campos de la gramática de eventos comunes, consulte la guía *Referencia de la gramática de eventos comunes* de la ayuda en línea.

Para ejecutar manualmente el proceso de CA IT PAM configurado de acuerdo con un fila de resultados de la consulta que se muestra

1. Haga clic en la ficha Consultas e informes y en la subficha Consultas.

Aparecen la lista de filtro de etiquetas de consulta y la lista de consultas.

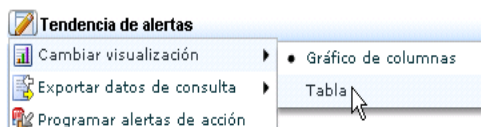
2. (Opcional) Introduzca criterios de búsqueda como, por ejemplo, cuentas predeterminadas, en la lista de consultas.

Los eventos que reflejan inicios de sesión por cuentas predeterminadas son buenos candidatos para transferencia al proceso de salida de alerta/evento de CA IT PAM.

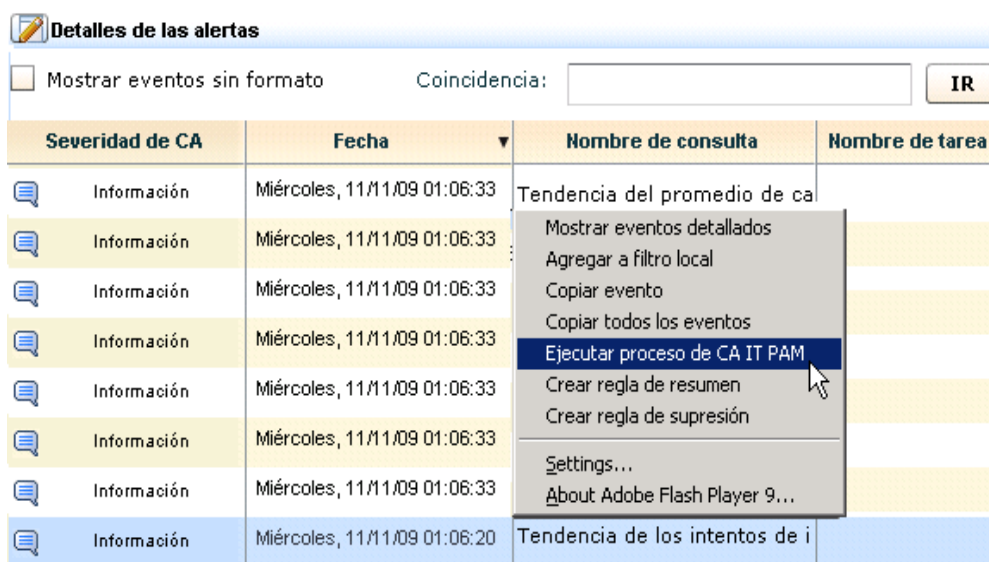
3. Seleccione la consulta en la lista de consultas de la que desee ver los resultados.

También puede mostrar la subficha Informes, seleccionar una opción de la lista de informes, cambiar a la vista de consulta individual y seleccionar la consulta en esta vista.

4. Si los resultados se muestran en un gráfico, seleccione Cambiar visualización en la lista desplegable de nombres de consultas y, a continuación, Tabla.



5. Seleccione la fila de resultados de la consulta para la que desee ejecutar el proceso de CA IT PAM.
6. Haga clic con el botón secundario del ratón en esta fila de resultados de la consulta y seleccione Ejecutar proceso de IT PAM en la lista desplegable.



Aparecerá el cuadro de diálogo Ejecutar proceso de IT PAM. Contiene el nombre y los parámetros del proceso definidos en la configuración de IT PAM del servicio del servidor de informes. Además, contiene la lista desplegable Seleccionar campo que permite introducir datos variables devueltos al campo de la gramática de eventos comunes seleccionado.

7. Rellene los campos como se indica a continuación:

- a. Revise los valores predeterminados que se muestran para los parámetros del proceso visualizados e identifique todos los valores que sea necesario modificar.

Estos parámetros y sus valores se obtienen de la configuración de integración de CA IT PAM.

- b. Para cambiar el valor predeterminado que se muestra, escriba el nuevo valor.
- c. Para especificar un valor variable, seleccione el campo de la gramática de eventos comunes en la lista desplegable Seleccionar campo que se encuentra en la parte superior del cuadro de diálogo y, a continuación, haga clic en Agregar campo, junto al cuadro de texto al que se refiera.
- d. En el caso de los campos que se encuentren en blanco, escriba un valor, seleccione una variable y agréguelo, o escriba una frase que incluya las variables seleccionadas.

Ejemplo de resumen: En (hora_fecha_evento), la cuenta (nombre_usuario_dest) ha realizado una acción (acción_evento) en el host (nombre_host_dest).

Ejemplo de descripción: El resultado de la acción (resultado_evento), se registra en el registro (nombre_registro_evento). La severidad de CA es (severidad_evento).

- e. Si el proceso de CA IT PAM especifica parámetros que hagan referencia a campos de la gramática de eventos comunes adicionales, seleccione estos campos en la lista que se muestra para enviarlos como parámetros.

A continuación, se muestra un ejemplo: La visualización puede incluir otros campos definidos en el proceso de salida de alerta/evento personalizado de IT PAM.

Ejecutar proceso de CA IT PAM

Proceso de IT PAM: /CA_ELM/EventAlertOutput

Seleccionar campo : event_severity

ReportedBy: ServiceDesk

Severity: 4

Priority: 3

EndUser: ServiceDesk

Summary: (event_action) action on the (dest_hostname) host.

Description: result, is logged in the (event_logname) log. The CA :

Enviar valores del campo como parámetros

☐ agent_address

☐ agent_connector_name

☐ agent_group

☐ agent_hostdomainname

☐ agent_hostname

☐ agent_id

☐ agent_name

Agregar campo

Aceptar Cancelar

8. Haga clic en Aceptar.

Aparecerá un cuadro de diálogo de progreso, seguido de un mensaje que indicará si el proceso de CA IT PAM se ha ejecutado correctamente y, de ser así, mostrará los resultados de la ejecución del proceso.

A continuación, se muestra un ejemplo en el que el resultado es Solicitud 4590 creada en el centro de servicio al usuario.



9. Haga clic en Aceptar.

10. Para ver los resultados en CA Service Desk, inicie sesión y busque "Solicitud" con el número del mensaje.

Por ejemplo, seleccione Solicitud e introduzca 4590.

Solicitud 4590

11. Aparecerán resultados de centro de servicio al usuario parecidos al siguiente.

Detalles de solicitud 80 Editar(\$) Crear orden de cambio Crear incidente(\$) Perfil rápido(0)

Usuario final afectado	Área de solicitud	Estado	Prioridad
ServiceDesk		Abierto	3

Detalles

Informado por	Asignatario	Grupo	Elemento de configuración
ServiceDesk	ServiceDesk		

Severidad	Urgencia	Impacto	¿Activo?
4-Escalación al gestor de Help Desk	4-Muy rápido	1-Toda la organización	SÍ

ID de cargo al usuario	Fecha/hora de devolución de llamada	Causa raíz

Cambio Causado por orden de cambio

Información de resumen

Resumen	Tiempo total de actividad
On Mon Aug 2009 11:58:59 AM, the su account performed a Alert Creation action on the ca-elm host.	00:01:28

Descripción
The action result S₁ is logged in the CALM log. The CA Severity is 2.

Fecha/hora de apertura	Última modificación	Fecha/hora de resolución	Fecha/hora de cierre
10/11/2009 15:57:31	10/11/2009 15:58:59		

12. Compare el resumen planificado y los datos de la descripción determinados en el paso 7 con los datos de la descripción que se muestran en Resumen de la información. Se incluyen datos de severidad de CA.

Diseño de consultas para eventos que se envían al proceso de salida de alerta/evento

Después de configurar la integración de CA IT PAM, puede realizar el primer paso para programar alertas que generen una salida de alerta/evento: compilación de una lista de consultas en las que se basarán las alertas. Generalmente son consultas para eventos que sugieren la infracción de una política. Puede utilizar una combinación de varios enfoques:

- Analizar las alertas programadas actualmente para identificar aquellas que deberían ejecutar el proceso de salida alerta/evento. Por ejemplo, si el proceso de salida de alerta/evento notifica una aplicación de departamento de asistencia técnica, identificará alertas que deberán abrir un parte del departamento de asistencia técnica.
- Analice sus políticas para identificar aquellas en las que se podría devolver una infracción a un evento registrados y, a continuación, cree una consulta para ese evento.
- Examine los resultados de otras consultas predefinidas para identificar datos que podría usar un producto de terceros como, por ejemplo, un producto de departamento de asistencia técnica, para adoptar una medida correctiva.
- Si el proceso de salida de alerta/evento de CA IT PAM crea partes en un producto de departamento de asistencia técnica de terceros, revise los tipos comunes de partes de departamento de asistencia técnica para encontrar las causas que se podrían capturar como registros de eventos.

Para identificar o diseñar consultas en las que se puedan basar alertas que ejecuten el proceso de salida de alerta/evento de CA IT PAM

1. Para cada tipo de evento que necesita un parte de departamento de asistencia técnica, identifique, modifique o cree una o varias consultas que capturen datos para ese tipo de evento.
 - Identifique cada consulta predefinida que recopile eventos sobre esas condiciones.
 - Si una consulta predefinida requiere personalización, copie la consulta y, a continuación, adapte la copia a sus necesidades.
 - Si no existe ninguna consulta predefinida para recopilar un tipo de evento determinado que requiera notificación del departamento de asistencia técnica, cree las consultas que necesite.
2. Para una consulta cualquiera que vaya a buscar un evento de TI en el que uno de los campos tenga alguno de varios valores conocidos, utilice una lista con clave predefinida, personalice la lista con clave o cree una nueva. Si los valores para esa clave existen en un archivo csv, impórtelos. En la caso de una lista generada mediante un proceso de IT PAM, configure ese proceso como el proceso de valores dinámicos, cree la clave y, a continuación, importe los valores de CA IT PAM.
3. Determine si se ejecutará el proceso de salida de alerta/evento de CA IT PAM para cada consulta que devuelva resultados o para cada fila de resultados.
4. Pruebe la consulta.
 - a. Cree la condición que genere el evento que desee capturar.
 - b. Ejecute la consulta o el conjunto de consultas de forma manual.
 - c. Evalúe si los resultados de la consulta son suficientes para que el personal del departamento de asistencia técnica realice el seguimiento necesario.
 - d. Si no es así, modifique la consulta o el conjunto de consultas para que proporcionen la información necesaria y vuelva a realizar la prueba.

Esta preparación garantiza que cuando se programe una alerta que ejecute la consulta o el conjunto de consultas, la salida de alerta/evento resultante contenga los datos necesarios para la resolución.

Más información:

[Personalización de consultas para las alertas de acción](#) (en la página 376)

Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por fila

Puede enviar una alerta que ejecute el proceso de salida de alerta/evento de CA IT por fila o por consulta. En este ejemplo se muestra el procedimiento necesario para ejecutar el proceso por fila. Incluye un ejemplo de lo que puede ver el personal que trabaja con CA IT PAM y con el producto de terceros al que CA IT PAM envía los detalles para este tipo de alerta.

Antes de crear una alerta para que ejecute un proceso de IT PAM para una consulta determinada, se recomienda identificar las columnas de gramática de eventos comunes que devuelven datos. Estas columnas son las que se seleccionan al crear un resumen y una instrucción de descripción para la alerta.

Nota: Copie la consulta y haga clic en el paso Columnas de la consulta. En el caso de los campos diseñados para que sean visibles, observe el nombre de la columna correspondiente al nombre para mostrar. Por ejemplo, el campo de la gramática de eventos comunes que se utiliza para rellenar la columna Cuenta es dest_username.

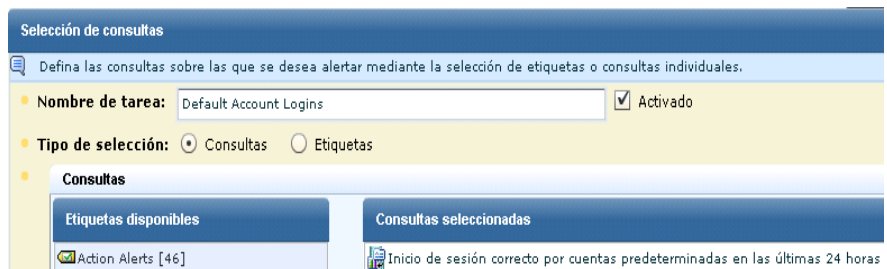
Columnas seleccionadas		
 		
Nombre para mostrar	Columna	Visible
Date	event_datetime	☒
Account	dest_username	☒
Host	dest_hostname	☒
Log Name	event_logname	☒
Action	event_action	☒
Result	event_result	☒

Para crear una alerta cuando los miembros de una cuenta predeterminada inician sesión correctamente

1. Haga clic en la ficha Gestión de alertas y, a continuación, haga clic en la subficha Programación de alertas.
2. Haga clic en Programar una alerta de acción.

Aparece el asistente de programación de alertas de acción.

3. Lleve a cabo el paso de selección de alertas según se indica a continuación:
 - a. Introduzca el nombre de la tarea, por ejemplo, Inicios de sesión de cuentas predeterminadas.
 - b. Haga clic en la etiqueta Alertas de acción.
 - c. Seleccione la consulta Inicio de sesión correcto por cuentas predeterminadas en las últimas 24 horas y desplácela a la lista de consultas seleccionadas.



4. Seleccione un intervalo de fechas para ejecutar la consulta y el número máximo de filas que se mostrará.
 - a. Haga clic en Condiciones de resultado.
 - b. Seleccione un intervalo de fechas como, por ejemplo, 'ahora' y 'ahora' '- 1 hora'.
 - c. Seleccione los parámetros para mostrar del resultado como, por ejemplo, límite de filas de 10 y granularidad de tiempo como event_datetime.
 - d. Omita los eventos agrupados.
5. Defina la programación.
6. Defina los datos de alerta que se transmitirán al proceso de IT PAM, junto con los datos de evento recuperados mediante la consulta.
 - a. Haga clic en el paso Destino.
 - b. Seleccione la ficha Proceso de IT PAM.
 - c. Seleccione Inicio de sesión correcto por cuentas predeterminadas en las últimas 24 horas.
 - d. Seleccione Ejecutar proceso de IT PAM por fila.
 - e. Si el proceso de IT PAM configurado no es el que desea ejecutar, cambie la ruta del proceso de IT PAM. El proceso de IT PAM debe contener la ruta completa que comienza por una barra diagonal (/).

- f. (Opcional) Cree una instrucción de resumen con texto literal y variables. En este caso, las variables se obtienen de los campos de la gramática de eventos comunes cuando se refinan los datos recopilados para una fila. A continuación, se muestra un ejemplo de la instrucción de resumen mediante el uso de variables.

La cuenta (dest_username) ha realizado la acción (event_action) en (dest_hostname)

La primera instrucción se crea como se indica a continuación:

- Escriba "La cuenta"
- Seleccione dest_username en la lista desplegable Seleccionar campo y, a continuación haga clic en + junto al campo Resumen.
- Escriba "ha realizado la acción"
- Seleccione event_action en la lista desplegable Seleccionar campo y, a continuación, haga clic en + junto al campo Resumen.
- Escriba "en"
- Seleccione dest_hostname en la lista desplegable Seleccionar campo y, a continuación, haga clic en + junto al campo Resumen.

- g. (Opcional) Cree una descripción con texto literal y texto obtenido de los campos de la gramática de eventos comunes. Seleccione el campo que desee en la lista desplegable Seleccionar campo y haga clic en +. Por ejemplo:

El registro (event_logname) muestra el resultado de (event_result) en (event_datetime)

El (event_result) de la (event_action) se ha registrado en el registro (event_logname).

El registro (event_logname) muestra la acción (event_action) que tuvo el resultado (event_result).

- h. Para Enviar valores del campo como parámetros, seleccione todos los campos de la gramática de eventos comunes que utilice el proceso de IT PAM especificado como un parámetro de proceso.

Nota: Dado que el proceso seleccionado no utiliza nombres de campos de la gramática de eventos comunes como parámetros, no se seleccionará ningún campo en este ejemplo. Para determinar si un proceso personalizado utiliza este tipo de parámetros, consulte la ficha Conjunto de datos del proceso de salida de alerta/evento de CA IT PAM.

Inicio de sesión correcto por cuentas predeterminadas en las últimas 24 horas

☒ Ejecutar proceso de CA IT PAM por fila

Proceso de CA IT : /CA_ELM/EventAlertOutput

Seleccionar campo: dest_hostname

ReportedBy: ServiceDesk

Severity: 4

Priority: 4

EndUser: ServiceDesk

Summary: The (dest_username) account performed the (event_

Description: The (event_logname) log shows the result of (event_

Enviar valores del campo como parámetros

☐ dest_hostname

☐ dest_username

☐ event_action

☐ event_datetime

☐ event_logname

☐ event_result

7. Seleccione un servidor.
8. Haga clic en Guardar y cerrar.
- La tarea aparece en la lista de tareas de alertas de acción.

Tareas de alerta de acción					
☐	Nombre de tarea	Activado	Servidor	Repetición	Fecha y hora de inicio
☐	Default Accounts Login	verdadero	caelm	5 minutos	Jueves, 05/11/09 13:24:44

9. Haga clic en Gestión de alertas, Eventos autocontrolados para ver los resultados. A continuación se muestra una vista parcial de las filas de información:

Acción	Resultado	Descripción del resultado
Resource Modify	S	Update RSSFeed Alert Name [login attempts] on reportServer [ca-elm] recurrence [5] recurrenceType [Minutes] was Successful.
Alert Creation	S	Alert job [Default Account Logins] created successfully.
Alert Job Setup	S	Schedule Action Query Alert Name [Default Account Logins] on reportServer [ca-elm] was Successful.

10. Haga clic en la subficha Alertas de acción de la ficha Gestión de alertas. Seleccione la alerta que haya programado para ver los resultados de la consulta.

Nombre de alerta		Categoría		Fecha	
Default Account Logins		Inicio de sesión correcto por cuentas predeterminadas en las últimas 24 horas		Jueves, 05/11/09 19:59:24	
Default Account Logins					
Alert name(Default Account Logins) Alert created by(su) Federated job(Yes) Tags (Action Alerts) Time Zone (America/New_York) Reports on successful login activity by user accounts listed in Default_Accounts keyed list during the last 24 hour time frame Rows Returned(1)					
Fecha	Cuenta	Host	Nombre de registro	Acción	Resultado
Jueves, 05/11/09 19:55:29	su	ca-elm	CALM	Login Attempt	S

11. Seleccione la ficha Eventos autocontrolados para obtener los resultados devueltos desde CA IT PAM.

A continuación se muestra un ejemplo parcial de un mensaje satisfactorio, en el que este mensaje aparece en los eventos autocontrolados para el servidor de informes. Observe el número de parte que aparece después de Resultados =.

Acción	Resultado	Descripción del resultado
Notification Creation	S	IT PAM process ran successfully. Results = [Request 631 created in CA Service Desk.]

12. (Opcional) Revise los resultados en CA Service Desk, como se muestra a continuación:
- Inicie sesión en CA Service Desk.
 - Seleccione Solicitud e introduzca el número del problema.
 - Haga clic en el vínculo del número de solicitud para revisar los detalles del problema y el resumen de la información.

Más información:

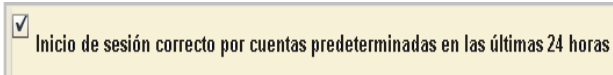
[Directrices para la creación de un proceso de alerta/evento](#) (en la página 407)

Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por consulta

Puede enviar una alerta que ejecute el proceso de salida de alerta/evento de CA IT por fila o por consulta. En este ejemplo se muestra el procedimiento necesario para ejecutar el proceso por consulta. Incluye un ejemplo de lo que puede ver el personal que trabaja con el producto de terceros al que CA IT PAM envía los detalles para este tipo de alerta.

Para enviar una alerta que ejecute el proceso de alerta/evento de CA IT PAM por consulta

1. Haga clic en la ficha Gestión de alertas y, a continuación, haga clic en la subficha Programación de alertas.
2. Haga clic en Programar una alerta de acción.
Aparece el asistente de programación de alertas de acción.
3. Lleve a cabo el paso de selección de alertas según se indica a continuación:
 - a. Introduzca el nombre de la tarea.
 - b. Seleccione una consulta.
4. (Opcional) Seleccione un intervalo de fechas para ejecutar la consulta y el número máximo de filas que se mostrará.
 - a. Haga clic en Condiciones de resultado.
 - b. Seleccione un intervalo de fechas como, por ejemplo, 'ahora' y 'ahora' '- 1 hora'.
 - c. Seleccione los parámetros que se desee mostrar del resultado.
5. Defina la programación.
6. Defina los datos de alerta que se transmitirán al proceso de IT PAM, junto con los datos de evento recuperados mediante la consulta.
 - a. Haga clic en el paso Destino.
 - b. Seleccione la ficha Proceso de IT PAM.
 - c. Seleccione la consulta que vaya a enviar.

A screenshot of a notification message box. It has a yellow background and a thin border. On the left side, there is a small square icon containing a checkmark. To the right of the icon, the text reads: "Inicio de sesión correcto por cuentas predeterminadas en las últimas 24 horas".

☒ Inicio de sesión correcto por cuentas predeterminadas en las últimas 24 horas

- d. Si desea que se informe de los resultados por consulta, deje en blanco Ejecutar proceso de IT PAM por fila.
- e. También puede escribir texto literal en los campos Resumen y Descripción.

- 7. Seleccione un servidor.
- 8. Haga clic en Guardar y cerrar.
La tarea aparece en la lista de tareas de alertas de acción.
- 9. Haga clic en la subficha Alertas de acción de la ficha Gestión de alertas.
Seleccione la alerta que haya programado para ver los resultados de la consulta.
- 10. Seleccione la ficha de eventos autocontrolados para la acción, Creación de notificación, con los resultados devueltos desde CA IT PAM. Un mensaje satisfactorio incluye el número de solicitud creado en la aplicación de terceros, si se trata de un producto de departamento de asistencia técnica.

Acción	Resultado	Descripción del resultado
Notification Creation	S	IT PAM process ran successfully. Results = Request 2936 created in CA Service Desk.

- 11. (Opcional) Para saber lo que ve el personal del departamento de asistencia técnica, revise los resultados de CA Service Desk como se indica a continuación:

- a. Inicie sesión en CA Service Desk.
- b. Seleccione Solicitud e introduzca el número que aparece en la descripción del resultado de Creación de notificación. Haga clic en Ir.

- c. Copia la dirección URL que aparece en la sección Resumen de la información y péguela en el explorador.



Aparecerá el cuadro de diálogo de inicio de sesión de CA Enterprise Log Manager.

- d. Inicie sesión en CA Enterprise Log Manager. Puede utilizar una cuenta con una función con privilegios bajos, como Auditor.

Los datos del evento devueltos por la consulta se presentan con el formato de la vista predeterminada de la consulta, es decir, tabla o gráfico.



Si se visualizan en formato de tabla, podrá ver datos del evento sin formato.

Más información:

[Configuración de destinos de las notificaciones](#) (en la página 479)

Trabajo con mensajes SNMP

Los sistemas de gestión de fallos y los centros de operaciones de la red (NOC) habitualmente reciben mensajes SNMP. Puede enviar alertas a este tipo de sistemas como mensajes SNMP v2 o mensajes SNMP v3, en función del producto de destino.

Las únicas tareas necesarias para trabajar con mensajes SNMP son las siguientes:

- Crear una MIB personalizada por cada alerta de acción para CA NSM.
- Preparar los productos de destino para la recepción de los mensajes de SNMP de CA Enterprise Log Manager.
- Programar alertas con uno o más destinos de mensaje SNMP.

La configuración del mensaje de SNMP predefinido de destino es opcional.

Acerca de los mensajes SNMP

SNMP es el acrónimo en inglés de Simple Network Management Protocol (Protocolo simple de administración de redes), un estándar abierto para el envío de mensajes de alerta a un destino especificado. Existen tres versiones de SNMP: SNMPv1, SNMPv2 y SNMPv3. CA Enterprise Log Manager puede emplear, tanto SNMPv2 como SNMPv3, a avisar a uno o varios sistemas de gestión de terceros cuando se produce un evento que genera una alerta.

En CA Enterprise Log Manager, se genera una alerta cuando una consulta programada devuelve resultados de las bases de datos del registro de eventos de los eventos refinados recientemente. Una consulta programada se puede configurar con mensaje SNMP como destino. Los receptores de mensajes, los sistemas de gestión de destino, pueden procesar mensajes a una velocidad de 200 mensajes por segundo aproximadamente. Generalmente, los receptores de mensajes SNMP escuchan en el puerto 162 de UDP, un puerto conocido para snmptrap.

CA Enterprise Log Manager le proporciona la flexibilidad que necesita para crear sus propias alertas personalizadas que puede enviar como mensajes SNMP. Por ejemplo, puede definir alertas para que se envíe una notificación cuando se produzca un evento crítico. También puede definir alertas para eventos como los cambios de configuración. Puede decidir qué alertas desea enviar como mensajes SNMP.

Ejemplo: filtros simples para alertas que se enviarán como mensajes SNMP

Los eventos que tienen un impacto negativo en determinadas operaciones, como el cierre de servicios, errores en los dispositivos o la supresión de recursos, resultan de interés para los centros de operaciones de red (NOC). Se pueden generar alertas de acción cuando se produzcan estos eventos y enrutarlos al NOC. Se pueden crear alertas personalizadas para esta finalidad si se emplean filtros simples en una solicitud personalizada. Tenga en cuenta los siguientes ejemplos de filtros simples.

- Error de dispositivo

Filtros simples	
Seleccione y disponga los filtros simples válidos	
☒ El modelo ideal es	Network Device
☒ La categoría del evento es	Operational Security
☒ La clase del evento es	Device and Port Activity
☒ La acción del evento es	Device Error

- Supresión de recursos

Filtros simples	
Seleccione y disponga los filtros simples válidos	
☒ El modelo ideal es	Network Management
☒ La categoría del evento es	Resource Access
☒ La clase del evento es	Resource Activity
☒ La acción del evento es	Resource Deletion

- Cierre del sistema

Filtros simples	
Seleccione y disponga los filtros simples válidos	
☒ El modelo ideal es	Operating System
☒ La categoría del evento es	Operational Security
☒ La clase del evento es	System Activity
☒ La acción del evento es	System Shutdown

Acerca de los archivos MIB

Los mensajes SNMP están definidos en archivos de base de información gestionada (MIB) estándar o MIB específicas de la empresa.

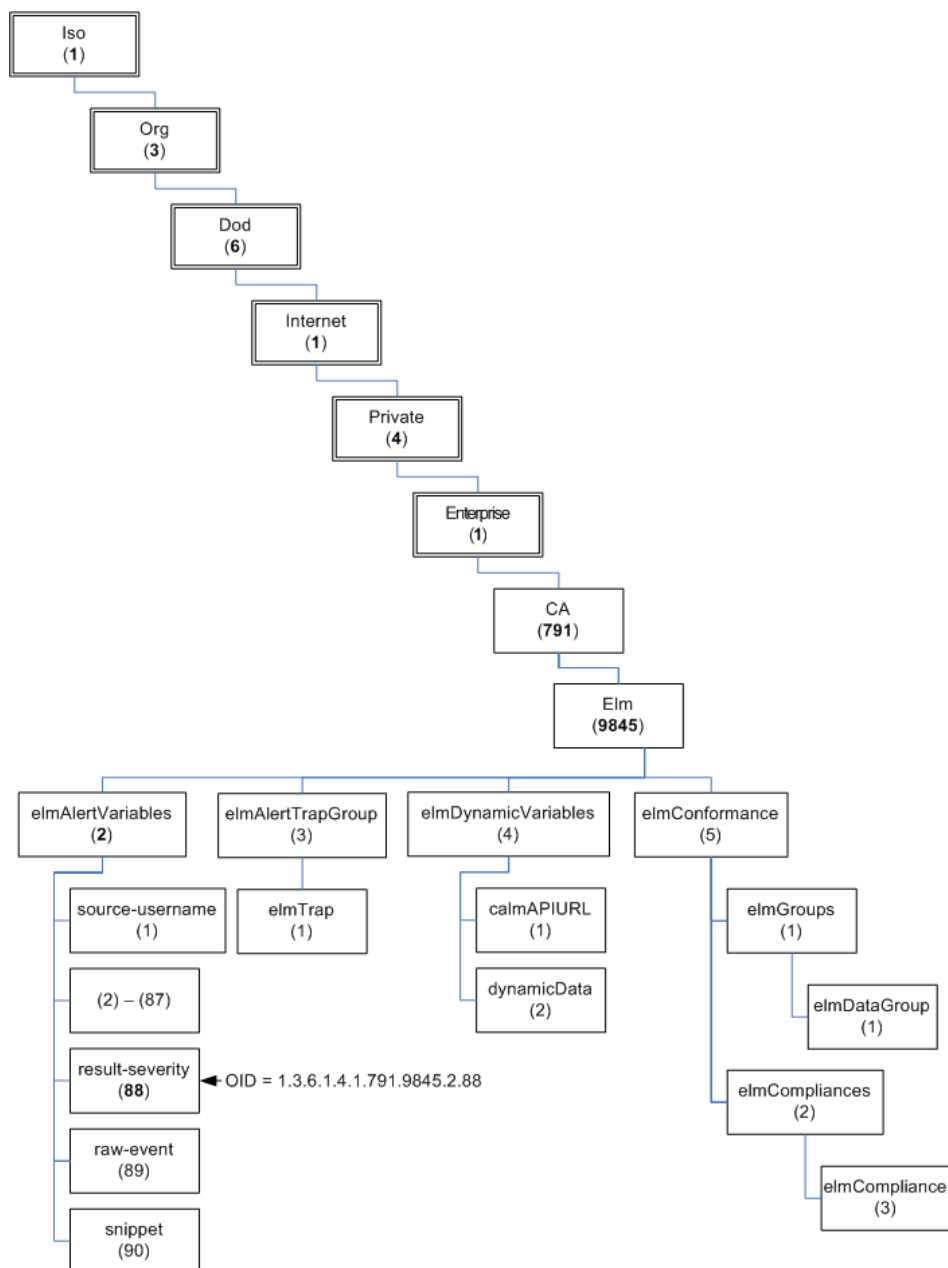
Cada empresa de la MIB tiene un número único que va precedido de los números de sus nodos principales. IANA ha asignado a CA, Inc. el número de empresa privada 791. Todos los datos enviados en mensajes SNMP por cualquier aplicación de CA están asociados con los ID de objeto que comienzan por 1.3.6.1.4.1.791. La aplicación de CA Enterprise Log Manager que pertenece a CA tiene el número 9845 como identificador. Todos los datos de mensajes SNMP enviados mediante alertas de acción de CA Enterprise Log Manager están asociados con ID de objetos (OID) que empiezan con 1.3.6.1.4.1.791.9845.

CA Enterprise Log Manager proporciona un archivo MIB. El nombre de esta MIB es CA-ELM.MIB. En esta MIB se definen todos los campos que pueden enviar las alertas de acción con un mensaje SNMP. Dicho mensaje SNMP incluye todos los campos de la gramática de eventos comunes que se encuentran disponibles en CA Enterprise Log Manager.

Cuando se envía una alerta de acción a un destino de mensaje SNMP, los datos enviados incluyen una URL. Los mensajes SNMP entrantes de control individuales pueden examinar la URL enviada por la alerta de acción. Al examinar la URL se abre una página de CA Enterprise Log Manager en la que se muestran los resultados de la consulta en un formato de fácil lectura. Esta funcionalidad acaba con la necesidad de usar MIB para interpretar los datos enviados como mensajes SNMP.

El árbol de la MIB de CA-ELM

Puede ver la estructura del archivo CA-ELM.MIB en el formato de árbol de MIB. Los campos de la gramática de eventos comunes se definen en elmAlertVariables con identificadores del objeto SNMP únicos. Por ejemplo, result_severity tiene un OID de 1.3.6.1.4.1.791.9845.2.88.



El archivo CA-ELM.MIB

El archivo MIB de CA Enterprise Log Manager, CA-ELM.MIB, se encuentra en el DVD de instalación. La MIB de CA Enterprise Log Manager se genera a partir del documento de origen de la gramática de eventos comunes, que contiene los OID para cada campo de la gramática de eventos comunes (elmAlertVariables).

El archivo CA-ELM.MIB comienza con la importación como se indica a continuación:

```
CAELM-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
        FROM SNMPv2-SMI
    MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
        FROM SNMPv2-CONF
        DisplayString
        FROM SNMPv2-TC;
```

La representación siguiente está diseñada para mostrar la estructura del árbol de MIB de CA Enterprise Log Manager, donde los nodos de nivel superior incluyen: iso(1) org(3) dod(6) internet(1) private(4) enterprises(1). El archivo CA-ELM.MIB real no tiene un formato como el que aparece en esta representación.

```
ca OBJECT IDENTIFIER ::= { enterprises 791 }
elm MODULE-IDENTITY... ::= { ca 9845 }
    elmAlertVariables ::= { elm 2 }
        source-username ::= { elmAlertVariables 1 }
        source-domainname ::= { elmAlertVariables 2 }
        source-groupname ::= { elmAlertVariables 3 }
        ...
        result-severity ::= { elmAlertVariables 88 }
        raw-event ::= { elmAlertVariables 89 }
        snippet ::= { elmAlertVariables 90 }
    elmAlertTrapGroup ::= { elm 3 }
        elmTrap ::= { elmAlertTrapGroup 1 }

    elmDynamicVariables ::= { elm 4 }
        calmAPIURL ::= { elmDynamicVariables 1 }
        dynamicData ::= { elmDynamicVariables 2 }
    elmConformance ::= { elm 5 }
        elmGroups ::= { elmConformance 1 }
            elmDataGroup ::= { elmGroups 1 }
        elmCompliances ::= { elmConformance 2 }
            elmCompliance ::= { elmCompliances 3 }
```

El archivo CA-ELM.MIB define un mensaje SNMP. Ese mensaje se define de la forma siguiente:

```
elmTrap NOTIFICATION-TYPE
    OBJECTS { source-username, source-domainname, source-groupname, source-
uid, source-gid, source-hostname, source-hostdomainname, source-address, source-mac-
address, source-port, source-processname, source-objectname, source-
objectattr, source-objectid, source-objectclass, source-objectvalue, dest-
username, dest-domainname, dest-groupname, dest-uid, dest-gid, dest-hostname, dest-
hostdomainname, dest-address, dest-mac-address, dest-port, dest-objectname, dest-
objectattr, dest-objectid, dest-objectclass, dest-objectvalue, agent-name, agent-
address, agent-hostname, agent-hostdomainname, agent-version, agent-id, agent-
connector-name, agent-group, event-source-hostname, event-source-
hostdomainname, event-source-address, event-source-processname, receiver-
name, receiver-hostname, receiver-hostaddress, receiver-hostdomainname, receiver-
port, receiver-time-gmt, receiver-timezone, receiver-version, event-protocol, event-
logname, event-euuid, event-count, event-summarized, event-duration, event-time-
year, event-time-month, event-time-monthday, event-time-weekday, event-time-
hour, event-time-minute, event-time-gmt, event-datetime, event-year-datetime, event-
month-datetime, event-day-datetime, event-hour-datetime, event-quarterhour-
datetime, event-minute-datetime, event-timezone, event-sequence, event-trend, event-
action, event-id, event-category, event-class, ideal-model, event-severity, event-
result, result-string, result-signature, result-code, result-version, result-
priority, result-scope, result-severity, raw-event, snippet }
    STATUS current
    DESCRIPTION
        El mensaje SNMP de ELM.
    ::= { elmAlertTrapGroup 1 }
```

El elmAlertTrapGroup es 1.3.6.1.4.1.791.9845.3 y el elmTrap está definido por el nodo siguiente. El ID predeterminado de elmTrap es 1.3.6.1.4.1.791.9845.3.1. Los ID de mensajes SNMP personalizados definidos por el usuario tienen el intervalo 1.3.6.1.4.1.791.9845.3.2 a 1.3.6.1.4.1.791.9845.3.999.

Importante: La mejor práctica para enviar mensajes a CA Spectrum es utilizar el ID de elmTrap predeterminado. La mejor práctica para enviar mensajes de SNMP a CA NSM es especificar un ID de mensaje personalizado que haga referencia al ID de un elmTrap en una MIB personalizada.

Asignación del ID de objeto (OID) al campo de la gramática de eventos comunes

En la tabla siguiente se muestra el campo de la gramática de eventos comunes que corresponda a cada Object ID (OID) de elmAlertVariables en el árbol de MIB. Esta rama del árbol crecerá a medida que se agreguen nuevos campos a la gramática de eventos comunes. Compruebe las actualizaciones de la MIB y asegúrese de que esté disponible la última versión para los productos de destino del mensaje SNMP.

ID de objeto (OID)	Campo de la gramática de eventos comunes
1.3.6.1.4.1.791.9845.2.1	source-username
1.3.6.1.4.1.791.9845.2.2	source-domainname
1.3.6.1.4.1.791.9845.2.3	source-groupname
1.3.6.1.4.1.791.9845.2.4	source-uid
1.3.6.1.4.1.791.9845.2.5	source-gid
1.3.6.1.4.1.791.9845.2.6	source-hostname
1.3.6.1.4.1.791.9845.2.7	source-hostdomainname
1.3.6.1.4.1.791.9845.2.8	source-address
1.3.6.1.4.1.791.9845.2.9	source-mac-address
1.3.6.1.4.1.791.9845.2.10	source-port
1.3.6.1.4.1.791.9845.2.11	source-processname
1.3.6.1.4.1.791.9845.2.12	source-objectname
1.3.6.1.4.1.791.9845.2.13	source-objectattr
1.3.6.1.4.1.791.9845.2.14	source-objectid
1.3.6.1.4.1.791.9845.2.15	source-objectclass
1.3.6.1.4.1.791.9845.2.16	source-objectvalue
1.3.6.1.4.1.791.9845.2.17	dest-username
1.3.6.1.4.1.791.9845.2.18	dest-domainname
1.3.6.1.4.1.791.9845.2.19	dest-groupname
1.3.6.1.4.1.791.9845.2.20	dest-uid
1.3.6.1.4.1.791.9845.2.21	dest-gid
1.3.6.1.4.1.791.9845.2.22	dest-hostname

ID de objeto (OID)	Campo de la gramática de eventos comunes
1.3.6.1.4.1.791.9845.2.23	dest-hostdomainname
1.3.6.1.4.1.791.9845.2.24	dest-address
1.3.6.1.4.1.791.9845.2.25	dest-mac-address
1.3.6.1.4.1.791.9845.2.26	dest-port
1.3.6.1.4.1.791.9845.2.27	dest-objectname
1.3.6.1.4.1.791.9845.2.28	dest-objectattr
1.3.6.1.4.1.791.9845.2.29	dest-objectid
1.3.6.1.4.1.791.9845.2.30	dest-objectclass
1.3.6.1.4.1.791.9845.2.31	dest-objectvalue
1.3.6.1.4.1.791.9845.2.32	agent-name
1.3.6.1.4.1.791.9845.2.33	agent-address
1.3.6.1.4.1.791.9845.2.34	agent-hostname
1.3.6.1.4.1.791.9845.2.35	agent-hostdomainname
1.3.6.1.4.1.791.9845.2.36	agent-version
1.3.6.1.4.1.791.9845.2.37	agent-id
1.3.6.1.4.1.791.9845.2.38	agent-connector-name
1.3.6.1.4.1.791.9845.2.39	agent-group
1.3.6.1.4.1.791.9845.2.40	event-source-hostname
1.3.6.1.4.1.791.9845.2.41	event-source-hostdomainname
1.3.6.1.4.1.791.9845.2.42	event-source-address
1.3.6.1.4.1.791.9845.2.43	event-source-processname
1.3.6.1.4.1.791.9845.2.44	receiver-name
1.3.6.1.4.1.791.9845.2.45	receiver-hostname
1.3.6.1.4.1.791.9845.2.46	receiver-hostaddress
1.3.6.1.4.1.791.9845.2.47	receiver-hostdomainname
1.3.6.1.4.1.791.9845.2.48	receiver-port
1.3.6.1.4.1.791.9845.2.49	receiver-time-gmt
1.3.6.1.4.1.791.9845.2.50	receiver-timezone

ID de objeto (OID)	Campo de la gramática de eventos comunes
1.3.6.1.4.1.791.9845.2.51	receiver-version
1.3.6.1.4.1.791.9845.2.52	event-protocol
1.3.6.1.4.1.791.9845.2.53	event-logname
1.3.6.1.4.1.791.9845.2.54	event-euuid
1.3.6.1.4.1.791.9845.2.55	event-count
1.3.6.1.4.1.791.9845.2.56	event-summarized
1.3.6.1.4.1.791.9845.2.57	event-duration
1.3.6.1.4.1.791.9845.2.58	event-time-year
1.3.6.1.4.1.791.9845.2.59	event-time-month
1.3.6.1.4.1.791.9845.2.60	event-time-monthday
1.3.6.1.4.1.791.9845.2.61	event-time-weekday
1.3.6.1.4.1.791.9845.2.62	event-time-hour
1.3.6.1.4.1.791.9845.2.63	event-time-minute
1.3.6.1.4.1.791.9845.2.64	event-time-gmt
1.3.6.1.4.1.791.9845.2.65	event-datetime
1.3.6.1.4.1.791.9845.2.66	event-year-datetime
1.3.6.1.4.1.791.9845.2.67	event-month-datetime
1.3.6.1.4.1.791.9845.2.68	event-day-datetime
1.3.6.1.4.1.791.9845.2.69	event-hour-datetime
1.3.6.1.4.1.791.9845.2.70	event-quarterhour-datetime
1.3.6.1.4.1.791.9845.2.71	event-minute-datetime
1.3.6.1.4.1.791.9845.2.72	event-timezone
1.3.6.1.4.1.791.9845.2.73	event-sequence
1.3.6.1.4.1.791.9845.2.74	event-trend
1.3.6.1.4.1.791.9845.2.75	event-action
1.3.6.1.4.1.791.9845.2.76	event-id
1.3.6.1.4.1.791.9845.2.77	event-category
1.3.6.1.4.1.791.9845.2.78	event-class

ID de objeto (OID)	Campo de la gramática de eventos comunes
1.3.6.1.4.1.791.9845.2.79	ideal-model
1.3.6.1.4.1.791.9845.2.80	event-severity
1.3.6.1.4.1.791.9845.2.81	event-result
1.3.6.1.4.1.791.9845.2.82	result-string
1.3.6.1.4.1.791.9845.2.83	result-signature
1.3.6.1.4.1.791.9845.2.84	result-code
1.3.6.1.4.1.791.9845.2.85	result-version
1.3.6.1.4.1.791.9845.2.86	result-priority
1.3.6.1.4.1.791.9845.2.87	result-scope
1.3.6.1.4.1.791.9845.2.88	result-severity
1.3.6.1.4.1.791.9845.2.89	raw-event

MIB personalizadas

Se pueden crear MIB personalizadas a partir del texto reutilizable si se agregan determinadas varbinds a partir del contenido del archivo CA-ELM.MIB. Un archivo personalizado para una alerta única contiene un subconjunto de contenidos del archivo CA-ELM.MIB. Las diferencias entre un archivo personalizado para una alerta y el archivo CA-ELM.MIB son las siguientes:

- La MIB personalizada define solamente los campos enviados por esa alerta.
- La MIB personalizada define un mensaje SNMP que muestra estos campos en la secuencia en la cual se envían.
- El mensaje SNMP de MIB personalizado se define con el OID, 1.3.6.1.4.1.791.9845.3.x, donde x es un valor entre 1 y 999.

Nota: Una alerta que utiliza una MIB personalizada especifica este OID como el valor de ID del mensaje SNMP personalizado.

- La MIB personalizada incluye la varbind `dynamicData` *solamente si* la consulta incluye campos calculados.

Los cálculos se pueden aplicar a cualquier campo. El campo `event_count` es un ejemplo de un campo al que habitualmente se aplican cálculos, aunque no es siempre así. En la consulta Recuento de eventos del sistema por acción de evento, `event_count` es un campo calculado que se calcula con `Sum`. Para determinar si un campo se calcula, se puede examinar la consulta en la que se define el campo. A continuación se muestra una definición en la que el campo `event_count` se calcula:

```
System_Event_Count_By_Event_Action.xml:    <Column columnname="event_count"
datatype="I" displayname="Count" functionname="sum" resultname="event_count"
sortdesc="true" sortorder="1" visible="true"/>
```

Texto reutilizable para MIB personalizadas

A continuación se muestra un texto reutilizable para una MIB personalizada. Si inicia una MIB personalizada con este ejemplo, podrá reemplazar o insertar datos personalizados en las ubicaciones indicadas con la cadena `###`. En las secciones donde se modifiquen datos es posible, opcionalmente, modificar la descripción.

```
CAELM-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
            FROM SNMPv2-SMI
        MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
            FROM SNMPv2-CONF
        DisplayString
            FROM SNMPv2-TC;
```

```
elm MODULE-IDENTITY
    LAST-UPDATED "200907050600Z"
    ORGANIZATION "CA"
    CONTACT-INFO
        "100 Staples drive
        Framingham MA"
    DESCRIPTION
        Contiene objetos que describen datos para eventos de ELM
    REVISION "200907050600Z"
    DESCRIPTION
        MIB personalizada <###>.
    ::= { ca 9845 }
```

```
ca OBJECT IDENTIFIER ::= {enterprises 791}
elmAlertTrapGroup OBJECT IDENTIFIER ::= { elm 3 }
elmAlertVariables OBJECT IDENTIFIER ::= { elm 2 }
elmDynamicVariables OBJECT IDENTIFIER ::= { elm 4 }
elmConformance OBJECT IDENTIFIER ::= { elm 5 }
elmGroups        OBJECT IDENTIFIER ::= { elmConformance 1 }
elmCompliances OBJECT IDENTIFIER ::= { elmConformance 2 }
```

<### Inserte una varbind de elmAlertVariable por cada campo de consulta ###>

<### Inserte la siguiente varbind de dynamicData sólo si la consulta incluye campos calculados ###>

```
dynamicData OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
```

Este campo contiene todas las variables dinámicas y datos de elm en el formato nombre=valor.

```
    ::= { elmDynamicVariables 2 }
```

```
calmAPIURL OBJECT-TYPE
    SYNTAX OCTET STRING
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
```

La URL OPEN API que se dirige al resultado de la consulta.

```
    ::= { elmDynamicVariables 1 }
```



```

elmTrap NOTIFICATION-TYPE
    OBJECTS { <### inserte una lista de campos de consulta con gui3n ###> }
    STATUS current
    DESCRIPTION
        El mensaje SNMP de ELM.
    ::= { elmAlertTrapGroup <### inserte el n3mero de nodo del ID de mensaje SNMP
personalizado ###> }

elmCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        La informaci3n de cumplimiento.
    MODULE -- this module
        GROUP      elmDataGroup
        DESCRIPTION
            Este grupo es obligatorio.
    ::= { elmCompliances 3 }
-- units of conformance

elmDataGroup    OBJECT-GROUP
    OBJECTS { <### inserte una lista de campos de consulta con gui3n ###> }
    STATUS current
    DESCRIPTION
        Una recopilaci3n de objetos que proporcionan informaci3n espec3fica
para
        los datos de ELM.
    ::= { elmGroups 1 }
END

```

Ejemplo: creaci3n de una MIB 33 personalizada para la consulta Tendencia del promedio de carga de la CPU

Cree una MIB personalizada para cada consulta enviada a CA NSM como un mensaje SNMP. Cada una de estas consultas est3 asociada con un ID de mensaje SNMP personalizado. La MIB personalizada define los campos seleccionados que se van a incluir en el mensaje, en el orden que se muestra en la alerta de acci3n.

Observe el ejemplo en el que la consulta seleccionada para la alerta de acci3n es Tendencia del promedio de carga de la CPU. Los campos seleccionados son event_datetime y event_trend.

Tendencia del promedio de carga de la CPU	
☒ Tendencia del promedio de carga de la CPU	Campos enviados al mensaje SNMP:
	☒ event_datetime
	☒ event_trend

El ID del mensaje SNMP personalizado es 1.3.6.1.4.1.791.9845.3.33.

Personalizar ID del mensaje SNMP: 1.3.6.1.4.1.791.9845.3.

Para crear una MIB personalizada para el ID de mensaje SNMP personalizado que termine en 33

1. Abra una copia de CA-ELM.MIB para poder copiar el texto en una MIB personalizada.
2. Abra un editor, copie el texto reutilizable para la MIB personalizada y guarde el archivo con un nombre nuevo. Por ejemplo, lo puede guardar como Custom MIB n.mib, donde n significa 33, el nodo final del ID de mensaje SNMP personalizado especificado para la consulta en la alerta de acción.
3. (Opcional) En elm MODULE-IDENTITY, sustituya <###> con 33. Por ejemplo:

Custom MIB 33."

4. Sustituya el siguiente texto reutilizable con texto de CA-ELM.MIB

<### Inserte la varbind de elmAlertVariable por cada campo de consulta en la secuencia de mensajes SNMP ###>

Copie las varbinds elmAlertVariable para event_datetime y para event_trend. Estas varbinds deben aparecer en la MIB y deben seguir la misma secuencia de envío que aparece en el mensaje SNMP. Por ejemplo:

```
event-datetime OBJECT-TYPE
    SYNTAX  DisplayString
    MAX-ACCESS  read-only
    STATUS    current
    DESCRIPTION
```

La fecha de calendario y la hora que se muestra en la información del evento
::= { elmAlertVariables 65 }

```
event-trend OBJECT-TYPE
    SYNTAX  Integer32
    MAX-ACCESS  read-only
    STATUS    current
    DESCRIPTION
```

Tendencia de los datos para este evento.
::= { elmAlertVariables 74 }

5. Ya que ninguno de los campos de esta consulta son campos calculados, borre el siguiente texto reutilizable.

```
<### Inserte la siguiente varbind de dynamicData sólo si la consulta incluye
campos calculados ###>
dynamicData OBJECT-TYPE
    SYNTAX  DisplayString
    MAX-ACCESS  read-only
    STATUS    current
    DESCRIPTION
    Este campo contiene todas las variables dinámicas y datos de elm en el
    formato nombre=valor.
    ::= { elmDynamicVariables 2 }
```

6. Sustituya el siguiente texto reutilizable en elmTrap:

```
OBJECTS { <### inserte una lista de campos de consulta con guión ###> }
con la lista de campos de consulta seleccionados, tal y como se muestra:
OBJECTS { event-datetime,event-trend }
```

7. Sustituya el siguiente texto reutilizable en elmTrap:

```
::= { elmAlertTrapGroup <### inserte el número de nodo del ID de mensaje SNMP
personalizado ###> }
por el siguiente:
::= { elmAlertTrapGroup 33 }
```

8. Sustituya el siguiente texto reutilizable en elmDataGroup:

```
OBJECTS { <### inserte una lista de campos de consulta con guión ###> }
por el siguiente:
OBJECTS { event-datetime,event-trend }
```

9. Guarde el archivo.

Ejemplo: MIB 33 personalizada

El ejemplo siguiente es una MIB 33 personalizada, desarrollada para una alerta de acción que se envía como un mensaje SNMP con el ID de mensaje SNMP personalizado terminado en 33. El ID del mensaje SNMP personalizado era 1.3.6.1.4.1.791.9845.3.33. La consulta seleccionada utiliza Tendencia del promedio de carga de la CPU y los campos seleccionados para el envío en el mensaje SNMP son event_datetime y event_trend.

```
CAELM-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
            FROM SNMPv2-SMI
        MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
            FROM SNMPv2-CONF
        DisplayString
            FROM SNMPv2-TC;

    elm MODULE-IDENTITY
        LAST-UPDATED "200907050600Z"
        ORGANIZATION "CA"
        CONTACT-INFO
            "100 Staples drive
            Framingham MA"
        DESCRIPTION
            "Contiene objetos que describen datos para eventos de ELM"
        REVISION "200907050600Z"
        DESCRIPTION
            "MIB personalizada 33."
        ::= { ca 9845 }

    ca OBJECT IDENTIFIER ::= { enterprises 791}
    elmAlertTrapGroup OBJECT IDENTIFIER ::= { elm 3 }
    elmAlertVariables OBJECT IDENTIFIER ::= { elm 2 }
    elmDynamicVariables OBJECT IDENTIFIER ::= { elm 4 }
    elmConformance OBJECT IDENTIFIER ::= { elm 5 }
    elmGroups OBJECT IDENTIFIER ::= { elmConformance 1 }
    elmCompliances OBJECT IDENTIFIER ::= { elmConformance 2 }

    event-datetime OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
            "La fecha de calendario y la hora que se muestra en la información del evento"
        ::= { elmAlertVariables 65 }
```

```
event-trend OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        Tendencia de los datos para este evento.
        ::= { elmAlertVariables 74 }

calmAPIURL OBJECT-TYPE
    SYNTAX OCTET STRING
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        La URL OPEN API que se dirige al resultado de la consulta.
        ::= { elmDynamicVariables 1 }

elmTrap NOTIFICATION-TYPE
    OBJECTS { event-datetime,event-trend }
    STATUS current
    DESCRIPTION
        El mensaje SNMP de ELM.
        ::= { elmAlertTrapGroup 33 }

elmCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        La información de cumplimiento.
    MODULE -- this module
        GROUP elmDataGroup
        DESCRIPTION
            Este grupo es obligatorio.
        ::= { elmCompliances 3 }
-- units of conformance

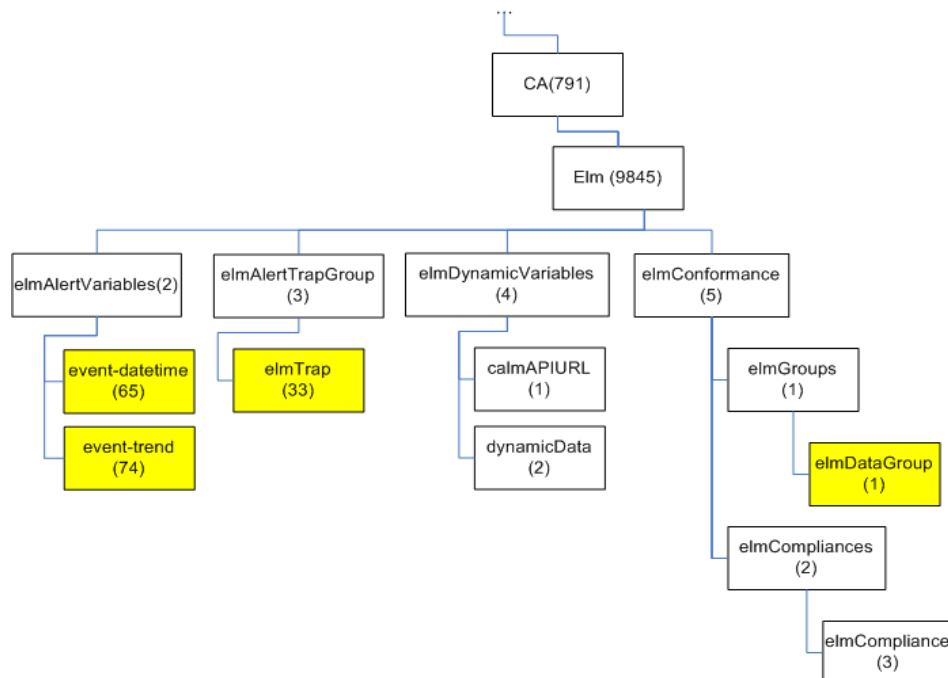
elmDataGroup OBJECT-GROUP
    OBJECTS { event-datetime,event-trend }
    STATUS current
    DESCRIPTION
        Una recopilación de objetos que proporcionan información específica
para
        los datos de ELM.
        ::= { elmGroups 1 }
END
```

Ejemplo: árbol de MIB para MIB 33 personalizada

El árbol de MIB de una MIB personalizada es diferente del árbol de MIB de CA-ELM.MIB en lo siguiente:

- Los objetos en elmAlertVariables están limitados por los campos que hay en la consulta. Observe el ejemplo en que los campos seleccionados son:
 - event_datetime
 - event_trend
- El elmTrap que contiene solamente los campos de consulta reemplaza elmTrap (1) en CA-ELM.MIB, que contiene todos los campos de la gramática de eventos comunes. Observe el ejemplo en que el elmTrap es 33. Este identificador de elmTrap hace referencia al nodo final del ID de mensaje SNMP personalizado, que es 1.3.6.1.4.1.791.9845.3.33.

A continuación se muestra una ilustración con una MIB 33 personalizada en formato de árbol de MIB. Los bloques resaltados indican diferencias entre esta MIB personalizada y CA-ELM.MIB. La MIB personalizada define solamente dos campos en elmAlertVariables. El elmTrap personalizado incluye sólo dos campos de consulta y tiene un número único, 33. elmDataGroup incluye solamente los dos campos de consulta.



Observaciones sobre el uso de MIB

Para que un sistema comprenda un mensaje SNMP recibido de CA Enterprise Log Manager mediante MIB, el sistema debe saber qué es lo que definen las OID que forman el mensaje. Los requisitos son los siguientes:

- Importe y recopile el archivo CA-ELM.MIB; mantenga actualizado este archivo.
- (Sólo para CA NSM) Cree, importe y recopile una MIB personalizada para cada alerta programada enviada como mensaje de SNMP.

Nota: Se puede utilizar la misma MIB personalizada con alertas basadas en consultas que envíen los mismos campos en el mismo orden en que lo hace un mensaje SNMP.

Por ejemplo, todas las consultas que se muestran a continuación devuelven valores para los campos `dest_hostname` y `event_count`.

- Cinco accesos al sistema erróneos por sistema
- Resumen de la actividad de restauración errónea en los últimos siete días por host
- Resumen de la actividad de copia de seguridad errónea en los últimos siete días por host
- Errores en la configuración durante la última hora excesivos (25)
- Cambios de configuración durante la última hora excesivos (25)
- Actividad SU por host durante la última hora excesiva (25)
- Resumen de los eventos críticos o graves en host crítico

Si se crean alertas separadas basadas en estas consultas, las alertas especificarán el mismo ID de mensaje SNMP personalizado y se interpretarán con la misma MIB personalizada.

Aquellas personas que controlan los mensajes SNMP recibidos en el producto de destino pueden interpretar los mensajes SNMP enviados por CA Enterprise Log Manager de dos formas:

- Mediante el inicio de la página de resultados de mensajes SNMP desde la URL enviada dentro del mensaje
- Mediante el uso de una aplicación que muestra una lista de las MIB importadas.

Proceso de trabajo con mensajes SNMP

El uso de mensajes SNMP implica los procedimientos siguientes:

1. Preparar CA Enterprise Log Manager para que envíe mensajes SNMP.
 - Configure el destino del mensaje SNMP predeterminado.
 - Identifique la dirección IP y el puerto de cada destino de mensaje SNMP adicional que se pueda determinar durante el envío de alertas como mensajes SNMP.
 - Identifique las alertas en las que los resultados de las consultas puedan ser de interés para CA Spectrum, CA NSM u otro receptor de mensajes SNMP.
2. Preparar los productos de destino del mensaje SNMP para que reciban mensajes SNMP desde CA Enterprise Log Manager.
 - Si el destino va a ser CA Spectrum:
 - Cree un modelo de evento de acuerdo con la documentación de Spectrum. Sin un modelo de evento, no puede ver los resultados de los mensajes SNMP en el destino.
 - Configure CA Spectrum para que pueda recibir mensajes SNMP v3.
 - Si el destino va a ser CA NSM:
 - Instale la versión NSM r11.2 GA en Windows Server 2003 EE SP1 y aplique el parche para actualizar el archivo aws_snmpex.dll.
 - Configure CA NSM para que reciba mensajes SNMP, incluidos los mensajes SNMP v3.

3. (Opcional) Preparar el destino del mensaje SNMP para que pueda interpretar los mensajes SNMP de CA Enterprise Log Manager con MIB.

- Descargue la MIB de CA Enterprise Log Manager en una ubicación accesible desde el producto de destino del mensaje SNMP.

Importante: CA-ELM.MIB está incluido en el DVD de instalación. Puede descargar la última versión de esta MIB desde la página de producto de CA Enterprise Log Manager.

- Importe y compile el archivo CA-ELM.MIB.
- (Solo para CA NSM) Por cada alerta que se enviará como mensaje SNMP, cree una MIB personalizada con un mensaje SNMP definido con 1.3.6.1.4.1.791.9845.3.x, donde x es un número entero igual o menor que 999. Importe y compile todas las MIB personalizadas.

Importante: Este paso es opcional ya que los mensajes SNMP recibidos de CA Enterprise Log Manager se pueden interpretar mediante el inicio de la página de resultados de mensajes SNMP desde la URL enviada en el mensaje SNMP.

4. Programar alertas con destinos de mensajes SNMP.
5. Comprobar que la alerta se ha enviado correctamente como un mensaje SNMP.
6. (Opcional) Controlar desde el destino del mensaje SNMP los resultados de los mensajes SNMP enviados.
 - Consulte los resultados de mensaje SNMP en el destino de mensaje SNMP.
 - Inicie la URL para ver los datos enviados por la alerta en formato de gráfico o tabla.

Configuración de la integración con un destino de trap de SNMP

Configure la integración de SNMP como parte de la configuración del servicio global para el servidor de informes. La configuración es la dirección IP y el puerto de un destino de trap de SNMP.

La integración de SNMP se puede configurar antes o después de preparar el producto de destino para que reciba e interprete traps de SNMP desde CA Enterprise Log Manager.

Cuando cree una alerta destinada a un destinatario de trap de SNMP, puede especificar uno o más destinos. Esta configuración sirve como el valor predeterminado. Este valor predeterminado se aplica a todos los servidores incluidos en el servidor de informes.

Para configurar la integración de SNMP

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Haga clic en servicio de alertas.
3. Introduzca la dirección IP o el nombre de host del servidor de destino para traps de SNMP.
4. Acepte el puerto predeterminado 162 o modifíquelo.
5. Haga clic en Guardar.

Preparación de CA Spectrum para recibir mensajes SNMP desde alertas

Puede enviar alertas en forma de mensajes SNMP de CA Enterprise Log Manager a cualquier destino de la red que capaz de recibir e interpretar mensajes SNMP. Cada producto receptor de mensajes SNMP tiene sus propios requisitos.

Prepare CA Spectrum para que pueda recibir mensajes SNMP de alertas de acción de CA Enterprise Log Manager haciendo lo siguiente:

- Cree una integración de puerta de enlace southbound de CA Spectrum, un punto de integración que admita cualquier formato de flujo de datos de alertas entrantes de un sistema de terceros, incluidos los mensajes SNMP como los que genera CA Enterprise Log Manager.
- Cree un modelo del nodo de CA Enterprise Log Manager para activar la recepción de mensajes SNMP v3.
- Descargue la MIB de CA Enterprise Log Manager.
- Importe la MIB de CA Enterprise Log Manager a CA Spectrum.

El proceso para crear una integración de puerta de enlace southbound aparece descrito por completo en *Spectrum Southbound Gateway Toolkit Guide*. La creación de una integración de puerta de enlace southbound incluye la asignación de mensajes SNMP a los eventos de CA Spectrum en un archivo AlertMap y la definición de los modelos necesarios. El punto de integración de puerta de enlace southbound admite datos de alerta de sistemas de terceros y los muestra en OneClick.

Después de descargar el archivo MIB de la página de producto de CA Enterprise Log Manager en CA Support Online o de recuperarlo del DVD de instalación, puede importarlo a CA Spectrum. Para obtener más información acerca del uso de la herramienta MIB para la importación en CA Spectrum OneClick, consulte *CA Spectrum Device Management User Guide*.

Configuración de CA Spectrum para que acepte mensajes SNMP v3

Para poder enviar mensajes SNMP V3 de CA Enterprise Log Manager a CA Spectrum, debe crear un modelo del dispositivo de CA Enterprise Log Manager en CA Spectrum. Los mensajes SNMP v3 se envían al nodo de CA Enterprise Log Manager que ha modelado.

Para crear un modelo que permita que Spectrum reciba mensajes SNMP v3 de las alertas de acción

1. Inicie sesión en servidor de Windows en el que se encuentra instalado CA Spectrum.
2. Acceda a la consola de Spectrum OneClick:
 - a. En el menú Inicio, haga clic en Todos los programas, CA, Panel de control de SPECTRUM.

El Panel de control de SPECTRUM aparece con un indicador Estado en la parte inferior de la pantalla.
 - b. Si en Estado no aparece EN EJECUCIÓN, haga clic en Iniciar SpectroSERVER en Control de proceso.
 - c. Si en Estado aparece EN EJECUCIÓN, haga clic en Administración de OneClick.

Administración de OneClick: en el panel de control de SPECTRUM, Host aparece como hostlocal y Puerto como 80.
 - d. Haga clic en Aceptar
Aparecerá un cuadro de diálogo de inicio de sesión.
 - e. Escriba sus credenciales.
Aparecerá la página SPECTRUM NFM OneClick.
 - f. Haga clic en Start Console.
El cuadro de diálogo Inicio de sesión: SPECTRUM OneClick aparecerá para conectar con SPECTRUM OneClick en el host local.
 - g. Haga clic en Aceptar
Consola: SPECTRUM OneClick aparecerá con un panel de navegación, un panel de contenido y un panel de detalles del componente.

3. En la ficha Explorador del panel de navegación, expanda el nodo de nivel superior y seleccione Universo.
En los títulos de los paneles de contenido y de detalles del componente, aparece Universo de tipo Universo.
4. En el panel de contenido, haga clic en la ficha Topología.
El segundo botón de la ficha le permite crear un nuevo modelo según el tipo y agregarlo a esta vista.
5. Haga clic en Crear un modelo nuevo.
Aparecerá el cuadro de diálogo Seleccionar tipo de modelo: SPECTRUM OneClick.
6. Haga clic en la ficha Todos los tipos de modelos.
7. Escriba una cadena en el campo Filtro. Por ejemplo, escriba gn.
Los tipos de modelo que empiecen por Gn aparecerán en la lista.
8. Seleccione el tipo de modelo que desee y haga clic en Aceptar. Por ejemplo, seleccione GnSNMPDev y haga clic en Aceptar.
Se abrirá Crear modelo de tipo <tipo de modelo seleccionado>.
9. Complete el cuadro de diálogo Crear modelo de tipo del siguiente modo:
 - a. Introduzca el nombre de host de un servidor de CA Enterprise Log Manager en el campo Nombre.
 - b. Escriba la dirección IP del mismo servidor en el campo Dirección de la red.
 - c. Escriba un puerto en el campo Puerto de agente, si el valor predeterminado 161 no es el que desea. Por ejemplo, introduzca 162.
 - d. Seleccione SNMP v3 como la opción Comunicación de SNMP.
 - e. Haga clic en Perfiles.La ventana Editar perfiles de SNMP v3 aparecerá con una lista de perfiles existentes, si existe alguno.

10. Para agregar un perfil, realice los siguientes pasos:

- a. Escriba el nombre de perfil y el ID del usuario.
- b. Ya que es una tarea para SNMP v3, seleccione Autenticación con privacidad como tipo de autenticación.
- c. En los siguientes cuatro campos, escriba una contraseña de autenticación de 8 caracteres dos veces y una contraseña de privacidad de 8 caracteres otras dos veces.
- d. Haga clic en Agregar para añadir el perfil a la lista.
- e. Haga clic en Aceptar.

El perfil que ha agregado aparece en primer lugar en la lista desplegable Perfil de V3 del cuadro de diálogo Crear modelo de tipo.

11. Seleccione Descubrir conexiones y haga clic en Aceptar.

Aparecerá el indicador de progreso Creando modelo. Una vez finalizado el procesamiento, el modelo creado aparecerá en la ficha Topología como un gráfico con el nombre de host que ha introducido y el tipo de modelo que ha seleccionado.

Descarga de la MIB de CALM

Puede descargar el archivo MIB desde la página de producto de CA Enterprise Log Manager en CA Support Online o recuperarlo del DVD de instalación. Después de descargar la MIB de CA Enterprise Log Manager, puede importarla o compilarla en todos los productos que configure como un destino de trap de SNMP.

Para descargar la MIB de CA Enterprise Log Manager

1. Inicie sesión en el servidor en el que haya instalado CA Spectrum.
2. Inicie CA Support Online e inicie sesión.
3. Acceda a la página de producto de CA Enterprise Log Manager.
4. Descargue el archivo MIB de CA Enterprise Log Manager en la red.
5. Si piensa enviar traps de SNMP a CA Spectrum, importe la MIB de CA Enterprise Log Manager a CA Spectrum.
6. Si piensa enviar traps de SNMP a CA NSM, importe la MIB de CA Enterprise Log Manager a CA NSM. Para conocer el procedimiento, consulte la documentación de CA NSM.

Importación de CAELM-MIB en CA Spectrum

Antes de enviar mensajes SNMP desde CA Enterprise Log Manager a CA Spectrum, puede importar y compilar la MIB de CA Enterprise Log Manager con las herramientas MIB de CA Spectrum OneClick.

Nota: Las MIB de SNMPv2 a las que se hace referencia en CA-ELM.MIB se cargan previamente en CA Spectrum.

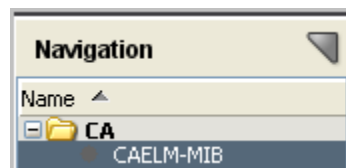
Para importar CA-ELM.MIB en CA Spectrum

1. Inicie sesión en CA Spectrum.
2. Inicie la consola de OneClick.
3. Haga clic en Herramientas, Utilidades, Herramientas MIB.
Se abrirá el cuadro de diálogo Herramientas MIB: Agregar MIB.
4. Haga clic en Examinar, desplácese hasta la ubicación en la que haya descargado CA-ELM.MIB y seleccione este archivo.
5. Haga clic en Compilar.

Aparecerá un mensaje que indicará que la MIB de CA Enterprise Log Manager se ha almacenado en el siguiente directorio del servidor Web de OneClick:

<\$SPECROOT>/MibDatabase/userContrib

6. Se cerrará el cuadro de diálogo Herramientas MIB: Agregar MIB.
CAELM-MIB se agregará a la barra de navegación de CA.



En la jerarquía, cai se expande para mostrar elm con los tres objetos subordinados y sus OID asociados.

Name	Object ID
cai	1.3.6.1.4.1.791
elm	1.3.6.1.4.1.791.9845
elmAlertVariables	1.3.6.1.4.1.791.9845.2
elmAlertTrapGroup	1.3.6.1.4.1.791.9845.3
elmDynamicVariables	1.3.6.1.4.1.791.9845.4
elmConformance	1.3.6.1.4.1.791.9845.5

Ejemplo: Alerta a CA Spectrum de cambios de configuración

Antes de enviar mensajes SNMP a CA Spectrum por primera vez, se recomienda identificar las consultas que devuelvan resultados apropiados para este destino. Al programar la primera alerta con Spectrum como, es posible que desee realizar el seguimiento de los resultados que se muestran en CA Enterprise Log Manager y compararlos con los que aparecen en la interfaz de CA Spectrum. Una vez que el envío de mensajes SNMP a CA Spectrum se convierta en una rutina, no será necesario que realice de nuevo estos pasos de preparación y seguimiento.

El ejemplo siguiente está diseñado para guiarle a lo largo del proceso inicial, e incluye las siguientes acciones:

- Preparación para el envío de mensajes SNMP a CA Spectrum
- Envío de mensajes SNMP a CA Spectrum
- Verificación de que los mensajes SNMP se han enviado correctamente
- Visualización de los mensajes SNMP recibidos mediante CA Spectrum

Más información:

[Envío de mensajes SNMPv2 a CA Spectrum](#) (en la página 456)

[Seguimiento del progreso de las tareas de alerta](#) (en la página 459)

[Visualización de traps de SNMP en CA Spectrum](#) (en la página 460)

Envío de mensajes SNMPv2 a CA Spectrum

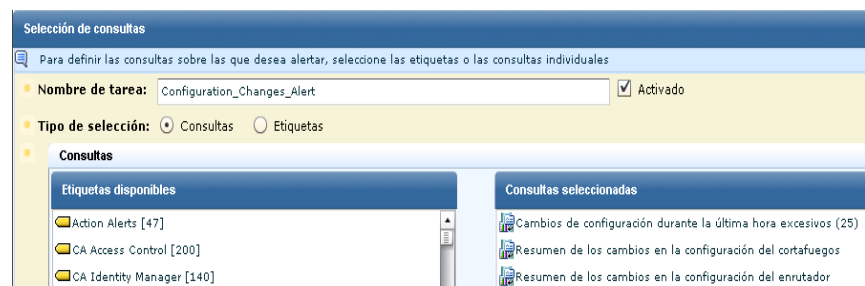
En el ejemplo siguiente se muestra el modo de crear una alerta que notifique a CA Spectrum los cambios de configuración con mensajes SNMPv2.

Para enviar mensajes SNMPv2 a CA Spectrum

1. Abra el asistente de programación de alertas.
 - a. Haga clic en la ficha Gestión de alertas y en la subficha Programación de alertas.
 - b. Haga clic en el botón Programar una alerta de acción.

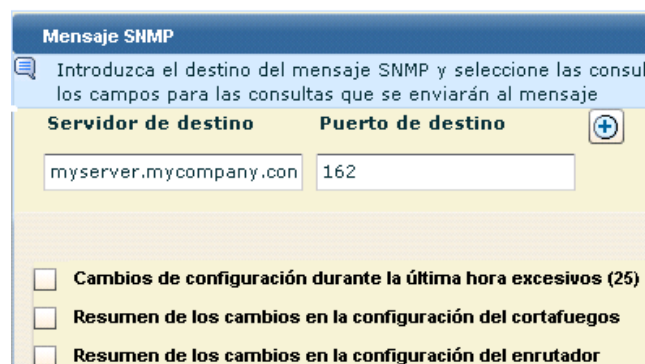
2. Lleve a cabo el paso Selección de alertas.
 - a. Escriba un nombre de tarea. Esta acción es obligatoria para cualquier alerta.
 - b. Verifique si el tipo de selección es Consultas.

No se permite seleccionar destinos de mensajes SNMP para alertas basadas en etiquetas.
 - c. Si las consultas que desea seleccionar están etiquetadas como alertas de acción, haga clic en la etiqueta Alertas de acción para filtrar la lista que se muestra.
 - d. Seleccione una o varias consultas que haya identificado.



3. (Opcional) Lleve a cabo los pasos Filtros de alerta, Condiciones de resultado y Programar tareas, de acuerdo con lo indicado en la ayuda en línea de este asistente.
4. Configure los detalles del mensaje SNMP.
 - a. Haga clic en el paso Destino.
 - b. Haga clic en la ficha Mensaje SNMP.

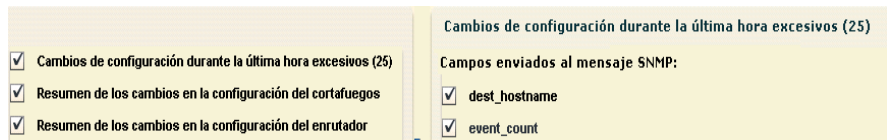
Aparecerá el destino del mensaje SNMP y las consultas seleccionadas en el paso 1 del asistente.



Nota: De manera predeterminada, SpectroSERVER escucha el puerto 162 del mensaje SNMP. Si se modifica, el puerto deberá coincidir con el parámetro snmp_trap_port del archivo SPECTRUM.vnmrc que se encuentra en el directorio SS.

- c. (Opcional). Para enviar el mensaje SNMP hasta a nueve servidores además de hacerlo al servidor de destino configurado, haga clic en el botón Agregar e introduzca la dirección IP y el puerto de destino del servidor.
- d. Para una consulta en la que desee que todos los campos se incluyan en el mensaje SNMP, sólo tiene que seleccionar la consulta.

Todos los campos de una consulta seleccionada se seleccionan de manera predeterminada. Aparecerá el nombre de la consulta seleccionada sobre la lista de campos.



Cambios de configuración durante la última hora excesivos (25)

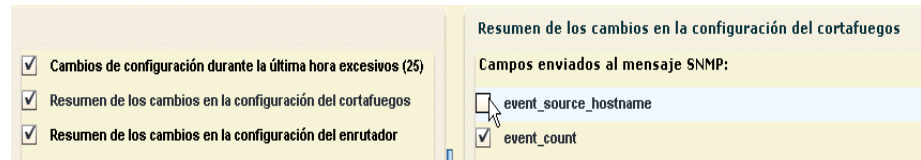
☒ Cambios de configuración durante la última hora excesivos (25)
☒ Resumen de los cambios en la configuración del cortafuegos
☒ Resumen de los cambios en la configuración del enrutador

Cambios de configuración durante la última hora excesivos (25)

Campos enviados al mensaje SNMP:

☒ dest_hostname
☒ event_count

- e. Para una consulta en la que desee que los campos seleccionados se incluyan en el mensaje SNMP, seleccione la consulta y borre los campos que no se vayan a enviar.



Resumen de los cambios en la configuración del cortafuegos

☒ Cambios de configuración durante la última hora excesivos (25)
☒ Resumen de los cambios en la configuración del cortafuegos
☒ Resumen de los cambios en la configuración del enrutador

Resumen de los cambios en la configuración del cortafuegos

Campos enviados al mensaje SNMP:

☐ event_source_hostname
☒ event_count

- f. Seleccione la versión de SNMP compatible con el destino del mensaje SNMP seleccionado para los mensajes SNMP recibidos de las aplicaciones.

Nota: Algunos destinos de los mensajes SNMP admiten mensajes SNMP de la versión 3 enviados directamente por los dispositivos pero sólo los mensajes SNMP de la versión 2 desde aquellas aplicaciones que recopilan eventos de dispositivos. En este ejemplo, se admite la versión 2.

- 5. Seleccione el servidor y especifique si la consulta sólo devolverá resultados de los servidores seleccionados o de este servidor y todos los servidores federados secundarios (si es una jerarquía) o iguales (si se encuentran en malla).

6. Haga clic en Guardar y cerrar.

La tarea aparece en la lista de tareas de alertas de acción. A menos que haya anulado la selección de la casilla de verificación Activado en el primer paso del asistente, se mostrará como Activado (verdadero en la columna Activado). A continuación, se muestra un ejemplo abreviado:

Tareas de alerta de acción								
☐	Nombre de tarea ▼	Activado	Servidor	Repetición	Fecha y hora de inicio	Hora de finalización	Zona horaria	Creador
☐	Configuration_Changes_Alert	verdadero	ca-elm	5 minutos	Miércoles, 11/11/09 00:56:08		America/New_York	su

Seguimiento del progreso de las tareas de alerta

Puede ver los resultados devueltos por las consultas seleccionadas para la alerta que ha creado. Los resultados que se muestran para el ejemplo Configuration_Changes_Alert aparecen en CA Enterprise Log Manager, debajo de los encabezados Host y Recuento.

1. Seleccione la ficha Gestión de alertas y la subficha Alerta de acción.
2. Haga clic en el nombre de alerta que haya programado.
3. Vea los resultados de esa alerta.

A continuación, se muestra un ejemplo de los resultados:

Nombre de alerta	Categoría	Fecha
Configuration_Changes_Alert	Cambios de configuración durante la última hora excesivos (25)	Jueves, 05/11/09 19:59:24
Configuration_Changes_Alert		
Alert name(Configuration_Changes_Alert) Alert created by(su) Federated job(Yes) Tags (Action Alerts) Time Zone (America/New_York) Lists Excessive Configuration Changes (more than 25) in last hour. Rows Returned(1)		
Host	Total	
ca-elm	2	

Visualización de traps de SNMP en CA Spectrum

Los traps de SNMP enviados mediante alertas de CA Enterprise Log Manager se pueden ver en el modelo de evento de CA Spectrum que creó para recibir estos traps. Los traps recibidos se muestran en la ficha Eventos. En el ejemplo Configuration_Changes_Alert, los resultados, ca-elm y 2, se muestran en CA Spectrum con los OID 1.3.6.1.4.1.791.9845.2.22 y 1.3.6.1.4.1.791.9845.2.2.

Para ver los traps de SNMP en CA Spectrum

1. Inicie sesión en CA Spectrum con sus credenciales de CA Spectrum.
2. Abra el Panel de control de Spectrum e inicie Spectroserver.
Se iniciará Spectroserver.
3. Haga clic en el administrador de OneClick e inicie sesión.
Aparecerá la aplicación Spectrum NFM OneClick.
4. Haga clic en Start Console.
Aparecerá la consola de Spectrum OneClick.
5. Expanda la carpeta creada para CA Enterprise Log Manager.
6. En Universe, seleccione el modelo de evento que creó para recibir los traps enviados desde CA Enterprise Log Manager.
7. En el panel de la derecha, seleccione la ficha Eventos para ver los traps enviados desde CA Enterprise Log Manager.

El valor, ca-elm y event_count=2 son los mismos datos que se pueden ver en CA Enterprise Log Manager.

A continuación se muestra un ejemplo no relacionado sobre cómo aparece un traps de SNMP enviado mediante una alerta de CA Enterprise Log Manager en CA Spectrum OneClick. El vínculo es la dirección URL que puede pegar en un explorador para que muestre la tabla de CA Enterprise Log Manager con los detalles en formato de gramática de eventos comunes.

Evento
Trap 6.1 received from unknown SNMP device with IP address 155.35.29.12 and community string 'public'. Trap identifier 1.3.6.1.4.1.791.9845.3. Trap var bind data: OID: 1.3.6.1.2.1.1.3.0 Value: 30000 OID: 1.3.6.1.6.3.1.1.4.1.0 Value: 1.3.6.1.4.1.791.9845.3.1 OID: 1.3.6.1.4.1.791.9845.2.65 Value: Tue Sep 22 2009 01:32:30 PM OID: 1.3.6.1.4.1.791.9845.2.44 Value: epSIM OID: 1.3.6.1.4.1.791.9845.2.45 Value: etr8511-blade7.ca.com OID: 1.3.6.1.4.1.791.9845.2.77 Value: Unknown Category OID: 1.3.6.1.4.1.791.9845.2.75 Value: Unknown Action OID: 1.3.6.1.4.1.791.9845.2.81 Value: Success OID: 1.3.6.1.4.1.791.9845.4.1 Value: <a ><param="" href="https://etr8511-blade7.ca.com:5250/spin/calmap/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/System_All_Events_Detail&params=;Params><Param id=ARG_stop val=1253606339,'unixepoch'" id="ARG_localtimezone" val='Asia/Calcutta"/></Params>"'>https://etr8511-blade7.ca.com:5250/spin/calmap/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/System_All_Events_Detail&params=;Params><Param id=ARG_stop val=1253606339,'unixepoch'"/><Param id=ARG_start val=1253606339,'unixepoch'"/><Param id=ARG_localtimezone val=Asia/Calcutta"/></Params>

Más información:

[Ejemplo: Alerta a CA Spectrum de cambios de configuración](#) (en la página 456)

Preparación de CA NSM para que reciba mensajes SNMP desde alertas

Puede enviar alertas en forma de mensajes SNMP de CA Enterprise Log Manager a cualquier destino de la red que capaz de recibir e interpretar mensajes SNMP. Cada producto receptor de mensajes SNMP tiene sus propios requisitos.

Para preparar CA NSM para que pueda recibir mensajes SNMP de alertas haga lo siguiente:

- Compruebe que el sistema CA NSM de destino cumple los requisitos necesarios para recibir datos de mensajes SNMP desde CA Enterprise Log Manager.
- Configure CA NSM para que reciba mensajes SNMP, lo que incluye la activación de la compatibilidad con SNMP v3, la modificación de las asignaciones de puertos en varios archivos y el inicio de los servicios necesarios.

Para preparar CA NSM para que pueda interpretar mensajes SNMP de alertas de acción haga lo siguiente:

- Cree una MIB personalizada para cada alerta que desea enviar a CA NSM como un mensaje SNMP.
- Importe y compile CA-ELM.MIB y todas las MIB personalizadas.

Requisitos del sistema de CA NSM

Si su sistema cumple los siguientes requisitos de la interfaz de CA Enterprise Log Manager, puede enviar mensajes SNMP a CA NSM:

- La versión de CA NSM es CA NSM r12.2 (versión GA).
- CA NSM está instalado en Windows Server 2003 EE SP1.
- Ha aplicado el parche T5MK056.caz, que actualiza el archivo aws_snmpex.dll y activa CA NSM para recibir mensajes SNMP v3 desde CA Enterprise Log Manager.

Para aplicar el parche

1. Descargue el parche de Soporte de CA.
2. Inicie sesión en el servidor con CA NSM.

3. Detenga el servicio Mensaje SNMP:
 - a. En el menú Inicio, seleccione Programas, Herramientas administrativas, Servicios.
Se abrirá la lista Servicios.
 - b. Seleccione el servicio Mensaje SNMP, haga clic con el botón secundario del ratón y seleccione Detener en el menú emergente.
4. Detenga todos los servicios de CA NSM:
 - a. Acceda al símbolo del sistema.
 - b. Introduzca el siguiente comando:
`Unicntrl stop all`
5. Copie el archivo del parche de descarga, "T5MK056.caz, en la carpeta C:\temp.
6. Descomprima el archivo del parche con cazipxp.
`Cazipxp.exe -u T5MK056.caz`
7. Realice una copia de seguridad del archivo aws_snmpex.dll antes de sustituirlo.
 - a. Desplácese a C:\Archivos de programa\CA\SC\CCS\AT\SERVICES\BIN.
 - b. Haga clic con el botón secundario del ratón en aws_snmpex.dll y seleccione Copiar.
Se agregará una copia del archivo aws_snmpex.dll a la carpeta.
8. Copie el archivo aws_snmpex.dll de la carpeta temp a la carpeta bin (C:\Archivos de programa\CA\SC\CCS\AT\SERVICES\BIN)
Ahora CA NSM cumple los requisitos del sistema. Puede configurar CA NSM para que reciba mensajes SNMP desde CA Enterprise Log Manager.

Configuración de CA NSM para que reciba mensajes SNMP

Antes de dirigir alertas para que se envíen a CA NSM como mensajes SNMP, deberá configurar CA NSM para que pueda recibir mensajes SNMP. Puede enviar, tanto mensajes SNMPv2 como mensajes SNMPv3 a CA NSM.

Para configurar CA NSM para que reciba mensajes SNMP desde alertas de CA Enterprise Log Manager

1. Inicie sesión en CA NSM.
2. Active la compatibilidad para SNMP version3, como se indica a continuación:
 - a. Muestre el símbolo del sistema. En el menú Inicio, haga clic en Ejecutar, introduzca cmd y haga clic en Aceptar.
 - b. Escriba lo siguiente:

```
caogui settings
```

Aparecerá la ventana Configuración de EM.
 - c. Haga clic en la ficha Gestión de eventos.
 - d. Desplácese para mostrar la descripción: SNMP - Activar la compatibilidad con la versión 3 de SNMP.
 - e. Seleccione la fila y escriba S para seleccionar Sí en la columna de configuración de SNMP, Activar la compatibilidad con la versión 3 de SNMP.
 - f. Haga clic en Sí para confirmar el cambio.
 - g. Cierre la ventana.

3. Cambie el puerto utilizado por el servicio SNMP del puerto actual, por ejemplo 5162, al puerto 162, como se indica a continuación:
 - a. Abra el Explorador de Windows.
 - b. Desplácese a la carpeta .../System32/drivers/etc que generalmente se encuentra en C:\WINDOWS.
 - c. Realice una copia de seguridad del archivo Servicios. Haga clic con el botón secundario del ratón en Servicios y seleccione Copiar.
 - d. Abra el archivo Servicios en un editor de texto como el Bloc de notas, y desplácese hasta la entrada que se parezca a la siguiente:

```
snmptrap    162/udp    snmp-trap    #SNMP trap
```

- e. Edite la línea snmptrap para sustituir el número de puerto 162 por un puerto alternativo como, por ejemplo, 5162. Agregue la línea catrapmuxd, en la que asignará el puerto 162.

```
snmptrap    5162/udp
catrapmuxd   162/udp    catrapmuxd   #CA Trap Multiplexer
```

- f. Guarde y cierre el archivo.
4. Modifique el archivo de configuración de CA Trap Multiplexer, catrapmux.conf, como se indica a continuación:
 - a. Desplácese a C:\Archivos de programa\CA\SC\CCS\WVEM\CAIUSER.
 - b. Abra CATRAPMUX.CONF mediante un editor de texto como el Bloc de notas.
 - c. Desplácese hasta el final del archivo. Edite el archivo como sea necesario para incluir las entradas siguientes.

```
CATRAPMUX_CMD:6161
AWS_SNMP:6162
catrapd:6163
snmptrap:5162
```

Nota: Las tres primeras entradas representan la configuración predeterminada.

- d. Guarde y cierre el archivo.

5. Agregue una línea al archivo de configuración snmpv3.dat para configurar los parámetros de seguridad de SNMP v3.

- a. Desplácese a C:\Archivos de programa\CA\SC\CCS\CommonResourcePackages\Misc.
- b. Abra el archivo snmpv3.dat en un editor de texto y agregue la línea siguiente al final del archivo.

```
*.*.*.* *.* test1234:AuthPriv:MD5:test1234:DES:test1234
```

Nota: Estos son los mismos parámetros que debe introducir en el cuadro de diálogo Parámetros de seguridad de V3 del asistente de alertas con el fin de que CA NSM reciba el mensaje SNMP. El nombre de usuario y la contraseña son los que se configuran aquí, el protocolo de Auth es MD5 y el protocolo de cifrado es DES.

- c. Guarde y cierre el archivo.

6. Instale el servicio CA Trap Multiplexer:

- a. Acceda al símbolo del sistema.
- b. Ejecute el siguiente comando:

```
catrapmuxd uniconfig
```

CA Trap Multiplexer se agregará a la lista de servicio con el estado Iniciado.

7. Verifique que CA Trap Multiplexer se esté ejecutando e inicie el servicio Mensaje SNMP.

- a. En el menú Inicio, seleccione Programas, Herramientas administrativas, Servicios.

Se abrirá la lista Servicios.

- b. Examine el estado de CA Trap Multiplexer. Verifique que el estado sea Iniciado.
- c. Seleccione el servicio Mensaje SNMP, haga clic con el botón secundario del ratón y seleccione Iniciar en el menú emergente.

8. Inicie todos los servicios con un tipo de inicio Automático.

- a. Acceda al símbolo del sistema.
- b. Ejecute el siguiente comando:

```
unicntrl start all
```

Ahora CA NSM estará configurado para recibir mensajes SNMP v3 basados en las alertas programadas enviadas por CA Enterprise Log Manager.

Ejemplo: cómo alertar a CA NSM acerca de los cambios en la configuración

El siguiente ejemplo está diseñado para ilustrar el proceso que se debe utilizar para alertar CA NSM acerca de los cambios en la configuración. Este proceso incluye los siguientes procedimientos:

- Envío de mensajes SNMP a CA NSM
- Comprobación de los mensajes SNMP que se han enviado correctamente
- Acceso a la consola de EM en CA NSM
- Visualización de los mensajes de SNMP recibidos por CA NSM.

Envío de mensajes SNMPv3 a CA NSM

Cuando se planifica qué alertas se enviarán a CA NSM es necesario identificar los resultados de las consultas que podrían ser de interés para el centro de operaciones de red. Por ejemplo, se deben tener en cuenta las consultas que detectan las modificaciones realizadas en la configuración. El siguiente ejemplo ilustra cómo enviar alertas programadas basadas en la consulta Detalles del cambio de configuración. Esta alerta especifica CA NSM como el destino de los mensajes SNMP.

para enviar mensajes SNMPv3 a CA NSM

1. Abra el asistente de programación de alertas.
 - a. Inicie sesión en CA Enterprise Log Manager con credenciales de Analyst o Administrator.
 - b. Haga clic en la ficha Gestión de alertas y en la subficha Programación de alertas.
 - c. Haga clic en el botón Programar una alerta de acción.
2. Lleve a cabo el paso Selección de alertas.
 - a. Introduzca un nombre de tarea. Por ejemplo, introduzca Cambios de configuración destinados a CA NSM.
 - b. Compruebe que el tipo de selección es Consultas. No se permite seleccionar destinos del mensaje SNMP para alertas basadas en etiquetas.
 - c. Seleccione una o varias consultas que haya identificado. Por ejemplo, seleccione Detalles del cambio de configuración.
3. (Opcional) Lleve a cabo los pasos Filtros de alerta, Condiciones de resultado y Programar tareas, de acuerdo con lo indicado en la ayuda en línea de este asistente.

4. Haga clic en el paso Destino y, a continuación, en la ficha Mensaje SNMP.
5. Examine las entradas de servidor y puerto de destino. Si no son correctos, introduzca la dirección IP del servidor y el puerto de destino. Para agregar servidores adicionales, haga clic en agregar e introduzca el destino adicional.
6. Especifique información de la versión de SNMP. De manera predeterminada, se selecciona la versión 2 de SNMP.

- a. Haga clic en la versión 3. Se configurará CA NSM para que pueda aceptar mensajes SNMP v3.
- b. Haga clic en Seguridad de V3.

Aparecerá el cuadro de diálogo Parámetros de seguridad de la versión 3 de SNMP.

Importante: Las entradas de este cuadro de diálogo deben coincidir con la configuración de snmpv3.dat que configuró para activar CA NSM de manera que pudiera recibir mensajes SNMP desde alertas de CA Enterprise Log Manager. A continuación, se muestra la configuración recomendada:

```
*.*.*.* *.* <nombreusuario>:AuthPriv:MD5:<contraseña>:DES:<contraseña>
```

- c. Seleccione Autenticación. Introduzca el nombre de usuario configurado para el nombre de usuario, la contraseña configurada para la contraseña, y seleccione MD5 para el protocolo.
- d. Seleccione Cifrado. Introduzca la contraseña configurada para la contraseña y seleccione DES para el protocolo.
- e. Haga clic en OK.

7. Seleccione la consulta que vaya a enviar como un mensaje SNMP.

En este ejemplo, si selecciona Detalles del cambio de configuración, los campos de esa consulta se mostrarán como se hayan seleccionado. También puede borrar los campos que no desee incluir como mensaje SNMP.

Importante: Cuando cree una MIB personalizada para esta alerta, asegúrese de que define un mensaje SNMP con los campos aquí seleccionados y en el siguiente orden:

The screenshot shows a web-based configuration interface. On the left, there is a list of configuration details with a checkbox next to 'Detalles del cambio de configuración', which is currently checked. On the right, under the heading 'Detalles del cambio de configuración', there is a section titled 'Campos enviados al trap de SNMP:'. Below this title, there is a list of fields, each with a checked checkbox: 'event_severity', 'event_datetime', 'dest_username', 'source_username', 'dest_hostname', 'event_logname', 'event_category', 'event_action', and 'event_result'.

8. Seleccione el número para el nodo final, x, del OID de elmTrap asociado, teniendo en cuenta que todos los OID de elmTrap se definen como 1.3.6.1.4.1.791.9845.3.x.

Los nodos iniciales del ID del mensaje SNMP personalizado están predefinidos en el archivo CA-ELM.MIB. El número de nodo final es único para cada mensaje SNMP definido en una MIB personalizada, en el que el mensaje SNMP refleja un conjunto único de campos. Un archivo MIB personalizado define los mensajes SNMP enviados por las alertas de CA Enterprise Log Manager que se hayan definido. En el mensaje SNMP personalizado, al cual hace referencia el ID de mensaje SNMP personalizado, los campos se muestran en el mismo orden que los campos enviados por la alerta. Si el OID para el mensaje SNMP en la MIB personalizada es 1.3.6.1.4.1.791.9845.3.63, seleccione 63 en el control de número como ID de mensaje SNMP personalizado. Por otro lado, si define la alerta en primer lugar, puede agregar un mensaje SNMP en la MIB personalizada para 1.3.6.1.4.1.791.9845.3.63 que define los campos de consulta seleccionados.

9. (Opcional) Seleccione Servidores.

10. Haga clic en Guardar y cerrar.

La tarea aparecerá en la lista Tareas de alerta de acción con el nombre de la tarea configurada.

Más información:

[Acceso a la consola de EM en CA NSM](#) (en la página 470)

Seguimiento del progreso de las tareas de alerta

Al programar una alerta, es recomendable realizar un seguimiento del progreso de las tareas de alerta la primera vez que se ejecuta. Al realizar un seguimiento del progreso, puede comprobar que la tarea se ejecute correctamente y que los resultados comunicados sean los que usted desee que se envíen.

Para controlar el progreso de las tareas de alerta y obtener una vista previa de los resultados.

1. Visualice la tarea de alerta que ha creado en la lista Tareas de alerta de acción. A continuación, se muestra un ejemplo parcial:

Tareas de alerta de acción					
☐	Nombre de tarea	Activado	Servidor	Repetición	Fecha y hora de inicio
☐	Configuration Changes destined for CA NSM	verdadero	ca-elm	5 minutos	Martes, 08/12/09 03:42:53

2. (Opcional) Para realizar el seguimiento del progreso de la tarea de alerta, vea Detalles de los eventos autocontrolados del sistema. Haga doble clic en cualquier línea para que aparezca el Visor de eventos. Desplácese hasta result_string para ver el mensaje completo que aparece en Descripción del resultado.

Acción	Resultado	Descripción del resultado
Notification Creation	S	SNMP trap for Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on report
Resource Creation	S	Creation of job file while executing action alert for Alert Name [Configuration Changes destined for CA NSM] was Successful.
Alert Creation	S	Run Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on reportServer [et
Resource Modify	S	Update RSSFeed Alert Name [Configuration Changes destined for CA NSM] on reportServer [etr65111f-sun104] recurrence [5
Resource Execution	S	Query [Configuration Change Detail] run over logDepot [localhost] was successful .

3. Obtenga una vista previa de los resultados devueltos por las consultas seleccionadas para la alerta que creó.
 - a. Seleccione la ficha Gestión de alertas y la subficha Alerta de acción.
 - b. Haga clic en el nombre de alerta que haya programado.
 - c. Ve a los resultados de esa alerta.

Nota: Generalmente, aquí se muestran los datos que aparecen al acceder a la URL enviada al servidor de destino. Si existe alguna diferencia y desea que sean iguales, edite la alerta de acción para restablecer la hora de finalización dinámica para Condiciones de resultado. Por ejemplo, establézcala en 'ahora, '-10 minutos'.

Acceso a la consola de EM en CA NSM

Puede ver los mensajes SNMP enviados mediante CA Enterprise Log Manager desde CA NSM. Los mensajes SNMP aparecen como mensajes en la consola de EM.

Para acceder a la consola de EM en CA NSM

1. Inicie sesión en el servidor en el que esté instalado el destino del mensaje SNMP, CA NSM.
2. En el menú Inicio, seleccione Programas, CA, Unicenter, NSM, Enterprise Management y EM Classic.

Aparecerá la ventana EM para Windows.
3. Haga doble clic en Windows.

Aparecerá la ventana del <nombrehost> (Windows).
4. Haga doble clic en Evento.

Aparecerá la ventana del <nombrehost> del evento (Windows).
5. Haga doble clic en los registros de consola.

Aparecerá la consola de EM (<nombrehost>).

Más información:

[Visualización de mensajes SNMP en CA NSM](#) (en la página 471)

Visualización de mensajes SNMP en CA NSM

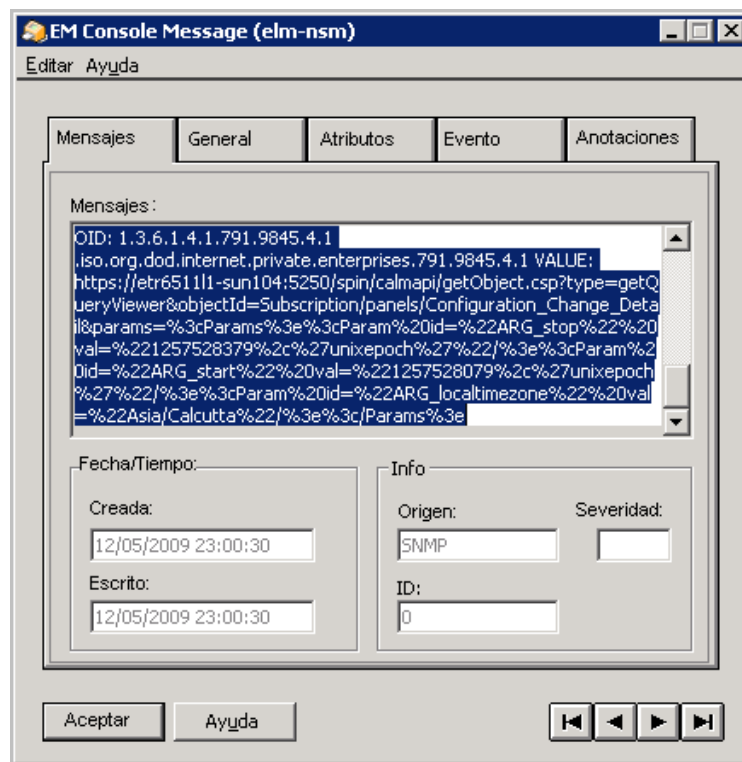
Tenga en cuenta el ejemplo en el que se programa una alerta para ejecutar la consulta Detalles del cambio de configuración. En este ejemplo, el ID de mensaje SNMP personalizado está configurado como 1.3.6.1.4.1.791.9845.3.63. Se envían nueve campos como mensaje SNMP.

Para ver el mensaje SNMP enviado por una alerta basado en la consulta Detalles del cambio de configuración

1. Cuando un evento autocontrolado indica que se ha enviado un mensaje SNMP a CA NSM, acceda a la consola de EM en CA NSM.
2. Espere hasta que aparezca un mensaje de registro que indique la recepción de un mensaje SNMP. El mensaje de este mensaje SNMP contiene el ID de mensaje SNMP personalizado, 1.3.6.1.4.1.791.9845.3.63.

```
%CATD_I_060, SNMPTRAP: -u auth user 791 155.35.7.63 etr6511l1-sun104.ca.com 6 63 0:05:00 12 OID: 1.3.6.1.2.1.1.3.0 system.sys
UpTime.0 VALUE: (30000) 0:05:00.00 OID: 1.3.6.1.6.3.1.1.4.1.0 .iso.org.dod.internet.snmpV2.snmpModules.1.1.4.1.0 VALUE: 1.3.6.1.
4.1.791.9845.3.63 OID: 1.3.6.1.4.1.791.9845.2.80 .iso.org.dod.internet.private.enterprises.791.9845.2.80 VALUE: 2 OID: 1.3.6.1.4.1
.791.9845.2.65 .iso.org.dod.internet.private.enterprises.791.9845.2.65 VALUE: Fri Nov 06 2009 10:53:53 PM OID: 1.3.6.1.4.1.791.9
%CATD_I_060, SNMPTRAP: -u auth user 791 155.35.7.63 etr6511l1-sun104.ca.com 6 63 0:05:00 12 OID:
```

- Haga doble clic en este mensaje para que aparezca el mensaje en un formato que puede copiar.



- Copie el mensaje y péguelo en un archivo de texto temporal.

El resultado es similar al siguiente:

```
%CATD_I_060, SNMPTRAP: -u auth user 791 155.35.7.63 etr6511l1-sun104.ca.com 6
63 0:05:00 12
```

Especifica que los siguientes datos se reciben como mensaje SNMP.

```
OID: 1.3.6.1.2.1.1.3.0 system.sysUpTime.0 VALUE: (30000) 0:05:00.00
```

Especifica el ID del objeto del tiempo de actividad en centésimas de segundo. Se trata de un OID conocido a través de un SNMP.

```
OID: 1.3.6.1.6.3.1.1.4.1.0 .iso.org.dod.internet.snmpV2.snmpModules.1.1.4.1.0
VALUE: 1.3.6.1.4.1.791.9845.3.63
```

Especifica el ID de objeto de snmpTrapOID. El valor es el ID de mensaje SNMP personalizado que especificó al configurar la alerta.

```
OID: 1.3.6.1.4.1.791.9845.2.80
.iso.org.dod.internet.private.enterprises.791.9845.2.80 VALUE: 2
```

Especifica el OID para event_severity el valor de severidad 2, que hace referencia a Informativo.

OID: 1.3.6.1.4.1.791.9845.2.65
.iso.org.dod.internet.private.enterprises.791.9845.2.65 VALUE: Fri Nov 06
2009 10:53:53 PM

Especifica el OID para event_datetime con el valor, el día, la fecha y la hora en los que se produjo el evento con estos valores.

OID: 1.3.6.1.4.1.791.9845.2.17
.iso.org.dod.internet.private.enterprises.791.9845.2.17 VALUE:

Especifica el ID de objeto para dest_username sin ningún valor.

OID: 1.3.6.1.4.1.791.9845.2.1
.iso.org.dod.internet.private.enterprises.791.9845.2.1 VALUE:

Especifica el ID de objeto para source_username sin ningún valor.

OID: 1.3.6.1.4.1.791.9845.2.22
.iso.org.dod.internet.private.enterprises.791.9845.2.22 VALUE: etr851l2-elm5

Especifica el ID de objeto para dest_hostname con el nombre de host del servidor en el que se muestran los resultados de la consulta al ejecutar la URL.

OID: 1.3.6.1.4.1.791.9845.2.53
.iso.org.dod.internet.private.enterprises.791.9845.2.53 VALUE: EiamSdk

Especifica el ID de objeto para event_logname, EiamSdk, el nombre del archivo de registro que contiene esta información.

OID: 1.3.6.1.4.1.791.9845.2.77
.iso.org.dod.internet.private.enterprises.791.9845.2.77 VALUE: Configuration
Management

Especifica el ID de objeto para event_category y el valor de Categoría asociado con la consulta Detalles del cambio de configuración.

OID: 1.3.6.1.4.1.791.9845.2.75
.iso.org.dod.internet.private.enterprises.791.9845.2.75 VALUE: Configuration
Change

Especifica el ID de objeto para event_action y el valor de Acción asociado con la consulta Detalles del cambio de configuración.

OID: 1.3.6.1.4.1.791.9845.2.81
.iso.org.dod.internet.private.enterprises.791.9845.2.81 VALUE: S

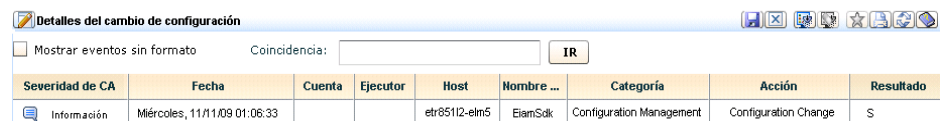
Especifica el ID de objeto para event_result con el valor, S (correctamente).

```
OID: 1.3.6.1.4.1.791.9845.4.1
.iso.org.dod.internet.private.enterprises.791.9845.4.1 VALUE:
https://etr651111-
sun104:5250/spin/calmap/api/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/Configuration_Change_Detail&params=%3cParams%3e%3cParam%20id=%22ARG_stop%22%20val=%221257528379%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_start%22%20val=%221257528079%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_local_timezone%22%20val=%22Asia/Calcutta%22/%3e%3c/Params%3e
```

Especifica el ID de objeto para calmAPIURL en elmDynamicVariables. El valor es la URL para la API de CA Enterprise Log Manager. Después de iniciar sesión, puede ver los resultados de la consulta en el gráfico o la vista de gráfico.

5. Copie la URL del final del mensaje, péguela en un explorador y ejecute la URL.
6. Inicie sesión en la API de CA Enterprise Log Manager.

Aparecerá la vista de gráfico de Detalles del cambio de configuración. Vea el ejemplo siguiente:



Severidad de CA	Fecha	Cuenta	Ejecutor	Host	Nombre ...	Categoría	Acción	Resultado
Información	Miércoles, 11/11/09 01:06:33			etr65112-elm5	EiamSdk	Configuration Management	Configuration Change	S

Creación de alertas de acción

El proceso de creación de una alerta de acción mediante el asistente de programación de alertas de acción consta de los siguientes pasos principales:

1. Apertura del asistente de programación de alertas de acción.
2. Selección de la consulta o las etiquetas en las que se basa la alerta. Puede consultar la base de datos de eventos, la base de datos de incidentes o ambas en una sola tarea.
3. (Opcional) Configuración de filtros avanzados para definir con más precisión la consulta de alerta.
4. (Opcional) Configuración de intervalo de fecha y condiciones del resultado
5. (Opcional) Definición de la frecuencia con la que se repite una tarea de alerta y cuándo está activa.
6. (Opcional) Configuración de los correos electrónicos de alerta automáticos y de los destinatarios.
7. (Opcional) Selección de si se ejecuta una consulta sobre datos sólo para el servidor seleccionado o si se ejecuta para dicho servidor y todos sus descendientes.

Más información:

[Apertura del asistente de programación de alertas de acción](#) (en la página 476)

[Creación de filtros de eventos avanzados](#) (en la página 597)

[Configuración de condiciones del resultado](#) (en la página 511)

[Configuración de destinos de las notificaciones](#) (en la página 479)

[Definición de destinos de las consultas de tareas de alerta](#) (en la página 485)

Apertura del asistente de programación de alertas de acción

Para crear una tarea de alerta de acción, debe emplear el asistente de programación de alertas de acción.

Para abrir el asistente de programación de alertas de acción

1. Haga clic en la ficha Gestión de alertas.
Aparece la lista de servidores de alertas.
2. Seleccione el servidor en el que desea programar una tarea de alerta.
El panel de detalles del servidor muestra el servidor seleccionado, en el que aparece la ficha de alertas generadas de forma predeterminada.
3. Haga clic en la ficha Programación de alertas y, a continuación, en el botón Programar alerta.
Aparece el asistente de programación de alertas de acción.
Al emplear el asistente:
 - Haga clic en Guardar y Cerrar para guardar la alerta de acción y cerrar el asistente.
 - Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Más información

[Configuración de destinos de las notificaciones de correo electrónico](#) (en la página 480)

[Definición de destinos de las consultas de tareas de alerta](#) (en la página 485)

Selección de consultas de alerta

Seleccione etiquetas o consultas como base para una nueva tarea de alerta de acción. La consulta, junto con los filtros que añada, define las circunstancias en las que se genera una alerta. Por ejemplo, para crear una alerta que controle el tráfico de un host o puerto, utilice la consulta de todos los eventos y añada filtros que definan los host de origen que desea controlar, así como un umbral de eventos.

Nota: La categoría de consultas de alertas de acción contiene consultas diseñadas para diversas necesidades de alertas comunes.

Para seleccionar consultas de alerta

1. Abra el asistente de programación de alertas de acción.
2. Introduzca un nombre de tarea.
3. Seleccione la zona horaria en la que desea programar el informe en el menú desplegable de zonas horarias.
4. Seleccione el botón de opción Consultas o Etiquetas para seleccionar los informes por etiqueta o de forma individual.

Nota: La programación de alertas por etiquetas le permite agregar alertas sin cambiar la tarea. Si selecciona la etiqueta "Gestión de identidades", todas las alertas que tengan esa etiqueta se añadirán a la tarea en el tiempo de ejecución programado. Puede agregar una alerta nueva a la tarea mediante la asignación de la etiqueta Gestión de identidades a una consulta. Esta función también se aplica a etiquetas personalizadas.

(Opcional) Anule la selección de la casilla de verificación Activar para activar la alerta de acción más tarde y no nada más terminarla. La casilla de verificación se encuentra seleccionada de forma predeterminada.

Nota: La capacidad para crear una tarea de alerta en estado desactivado está prevista para el uso con alertas repetidas. Si anula la selección de la casilla de verificación Activado correspondiente a una tarea y crea la tarea con una sola repetición ("Ahora" o "Una vez"), dicha tarea se eliminará de la lista de alertas programadas.

5. (Opcional) Seleccione una o varias etiquetas para limitar las etiquetas e informes individuales mostrados. Esta función coincide con el comportamiento de la lista de informes.
6. Seleccione las etiquetas o las consultas individuales que desee y utilice el control de cambio para agregarlas al área Consultas seleccionadas. Puede seleccionar tanto consultas de eventos como de incidentes en una sola tarea de alerta.

7. Vaya al paso de programación que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la tarea de alerta se programará; si no es así, aparecerá el paso que haya seleccionado.

Más información:

[Creación de filtros de eventos avanzados](#) (en la página 597)

[Configuración de condiciones del resultado](#) (en la página 511)

Establecimiento de parámetros de programación de tareas de alerta

Puede controlar cuándo aplicar las alertas mediante la definición de la hora de inicio y finalización. También puede controlar la granularidad de la visualización de las alertas mediante el control de la frecuencia de repetición de la consulta.

Para establecer los parámetros de programación de tareas de alerta

1. Abra el asistente de programación de alertas de acción, introduzca la información necesaria y vaya al paso de programación de tareas.
2. Establezca el intervalo de repetición deseado. Un intervalo más pequeño ofrece una visión más detallada, pero aumenta el tráfico en la red.

Antes de establecer un intervalo bajo, compruebe que CA Enterprise Log Manager esté sincronizado con un servidor de NTP.
3. Establezca la hora de inicio y finalización deseada para la tarea de alerta.
4. Vaya al paso de programación que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la tarea de alerta se programa; si no es así, aparece el paso que haya seleccionado.

Configuración de destinos de las notificaciones

Puede establecer uno o varios de los siguientes destinos para notificar una alerta:

- Correo electrónico

Puede establecer una notificación de correo electrónico automática para una alerta, con el fin de asegurarse de que el personal adecuado sea consciente de las alertas relacionadas con su función o responsabilidad con respecto a la tarea. Configure un servidor de correo para el entorno de CA Enterprise Log Manager antes de enviar correos electrónicos de notificación de alertas.

- Proceso de IT PAM

Puede ejecutar el proceso específico de CA IT PAM si la alerta se refiere a una condición que requiere notificación del producto de terceros. La integración con CA IT PAM se debe configurar en el servidor de informes, y se debe haber definido el proceso de IT PAM antes de ejecutar el proceso a partir de las alertas.

- Mensaje SNMP

Puede enviar datos de eventos capturados mediante una alerta a uno o varios centros de operaciones de la red (NOC). Puede dirigir servidores de gestión como, por ejemplo, CA Spectrum o CA NSM mediante el uso de mensajes SNMP v2 o SNMP v3. Los destinos se pueden especificar durante el proceso de programación de la alerta. Antes de enviar alertas mediante SNMP, se debe configurar la integración con SNMP.

Nota: Si no establece un destino, los resultados de la alerta sólo se publicarán en la fuente RSS.

Más información:

[Configuración de destinos de las notificaciones de correo electrónico](#) (en la página 480)

[Configuración de la información de CA IT PAM](#) (en la página 481)

[Ejemplo: Alerta a CA Spectrum de cambios de configuración](#) (en la página 456)

[Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por fila](#) (en la página 421)

[Ejemplo: Envío de una alerta que ejecute un proceso de IT PAM por consulta](#) (en la página 426)

Configuración de destinos de las notificaciones de correo electrónico

Puede establecer una notificación de correo electrónico automática para una tarea de alerta, de modo que se puede asegurar de que el personal adecuado es consciente de las alertas relacionadas con su rol o responsabilidad. Este paso es opcional.

Debe configurarse un servidor de correo electrónico para el entorno de CA Enterprise Log Manager para que pueda establecer notificaciones de correo electrónico de alertas.

Para configurar notificaciones de alertas

1. Abra el Asistente de programación de alertas de acción, introduzca la información necesaria y vaya al paso Destino.
2. Seleccione la casilla de verificación de activación de la notificación de correo electrónico.
3. Introduzca al menos una dirección de correo electrónico de destino. Puede introducir múltiples direcciones separadas por comas.
4. (Opcional) Introduzca el remitente, la línea de asunto y el cuerpo del mensaje del correo electrónico de notificación.

Nota: El cuerpo del mensaje se crea en formato HTML, por lo que todo el texto aparece en una línea. Para crear un salto de línea, introduzca
 al final de la línea de texto.

Más información:

[Configuración de la información de CA IT PAM](#) (en la página 481)

Configuración de la información de CA IT PAM

La tarea de alerta se puede configurar para que ejecute un proceso de CA IT PAM cuando se genera una alerta.

Puede ejecutar el proceso una vez para cada fila de resultados de la consulta o configurar el proceso una vez, independientemente del número de filas. Si ejecuta el proceso una vez por fila, defina instrucciones de resumen y descripción mediante los campos de la gramática de eventos comunes para enviar los datos de evento a CA IT PAM. Seleccione los campos que se hayan definido para recopilar datos mediante la consulta. Si lo ejecuta una vez por consulta, se enviará a CA IT PAM que, cuando se inicie, mostrará todas las filas de datos de evento. En el producto de terceros que responda al proceso CA IT PAM, la dirección URL se agregará al texto de resumen que introduzca. Por ejemplo, aparecerá en el campo Resumen de CA Service Desk, si es el producto de terceros.

Para ejecutar un proceso de CA IT PAM cuando se genera la alerta

1. Abra el asistente de programación de alertas de acción, introduzca la información necesaria y vaya al paso de destino.
2. Haga clic en la ficha Proceso de IT PAM.
En el panel izquierdo aparecerá una casilla de verificación para cada consulta de esta tarea de alerta.
3. Seleccione una consulta que desee enviar al proceso de CA IT PAM y realice una de las acciones siguientes:
 - Seleccione Ejecutar proceso de IT PAM por fila para ejecutar el proceso configurado una vez para cada fila devuelta.
 - Cancele la selección de Ejecutar proceso de IT PAM por fila para ejecutar el proceso configurado una vez, independientemente del número de filas devueltas.
4. Verifique las entradas predeterminadas para los parámetros del proceso y modifíquelas si es necesario. En los campos no definidos que permiten la entrada de información de resumen o descripción, introduzca una instrucción significativa. Si selecciona Ejecutar proceso por fila, utilice los campos de la gramática de eventos comunes para transmitir datos del evento. Seleccione el campo de la gramática de eventos comunes y haga clic en Agregar junto al campo de destino.
5. Si el proceso de CA IT PAM se define con campos de la gramática de eventos comunes como parámetros locales del conjunto de datos, seleccione los campos de la gramática de eventos comunes en la lista Enviar valores del campo como parámetros.

6. Seleccione otra consulta en el panel izquierdo y repita los pasos 3 a 6.

Nota: Si las consultas de una tarea de alerta programada devuelven resultados, toda la información y los parámetros necesarios para ejecutar el proceso configurado se enviarán a CA IT PAM.

Más información:

[Configuración de destinos de las notificaciones de correo electrónico](#) (en la página 480)

Configuración de la información de mensaje SNMP

Puede configurar el mensaje SNMP para que éste informe de una tarea de alerta, lo que le permitirá enviar la alerta a uno o varios sistemas de gestión de terceros. Cuando las consultas seleccionadas devuelven resultados, se envía un mensaje que incluya datos devueltos para todos los campos seleccionados de todas las consultas seleccionadas a todos los destinos de mensaje SNMP seleccionados. Este paso es opcional.

Para configurar información del mensaje SNMP

1. Abra el Asistente de programación de alertas de acción, introduzca la información necesaria y vaya al paso Destino.
2. Seleccione la ficha Mensaje SNMP.
Se abrirá la ficha Mensaje SNMP que mostrará los campos Servidor de destino y Puerto de destino, así como una lista de las consultas incluidas en la alerta de acción, cada una de ellas con una casilla de verificación.
3. Examine el servidor de destino predeterminado y las entradas de puerto. Si no son correctos, introduzca la dirección IP correcta o el nombre de host completo y el número de puerto.
4. (Opcional) Haga clic en Agregar para introducir el servidor de destino y los puertos de destino adicionales.
5. (Opcional) Para enviar la alerta mediante SNMP v3, seleccione la versión 3 de SNMP. La versión 2 de SNMP es el valor predeterminado.
6. Si selecciona la versión 3 de SNMP, haga clic en el botón Seguridad de V3 para configurar la autenticación o el cifrado en el cuadro de diálogo Parámetros de seguridad.

Importante: Las entradas de este cuadro de diálogo deben coincidir con la configuración de snmpv3.dat que configuró para activar CA NSM de manera que pudiera recibir mensajes SNMP desde alertas de CA Enterprise Log Manager. A continuación, se muestra la configuración recomendada:

```
*.*.*.* *.* <nombreusuario>:AuthPriv:MD5:<contraseña>:DES:<contraseña>
```

- a. Seleccione Autenticación. Introduzca el nombre de usuario configurado para el nombre de usuario, la contraseña configurada para la contraseña, y seleccione MD5 para el protocolo.
- b. Seleccione Cifrado. Introduzca la contraseña configurada para la contraseña y seleccione DES para el protocolo.

7. Seleccione la casilla de verificación junto a cualquier consulta que desee incluir en el mensaje SNMP. Por ejemplo, si tiene tres consultas que aparecen en la lista, puede configurar SNMP para que proporcione una, dos o las tres consultas.

Al seleccionar una consulta se muestran los campos incluidos en cada consulta, y cada una de ellas con una casilla de verificación seleccionada. Puede borrar cualquier campo seleccionado para eliminarlo de la alerta.

8. Introduzca el ID de mensaje SNMP personalizado que desee asociar con cada consulta. Esto le permite enviar consultas diferentes en una sola alerta a ID de mensaje SNMP diferentes, si necesario.
9. Vaya al paso de programación que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la tarea de alerta se programará; si no es así, aparecerá el paso que haya seleccionado.

Más información:

[Configuración de destinos de las notificaciones de correo electrónico](#) (en la página 480)

[Configuración de la información de CA IT PAM](#) (en la página 481)

Definición de destinos de las consultas de tareas de alerta

Puede seleccionar qué sistemas de almacenamiento de registro de eventos federados reciben consultas por parte de la tarea de alerta.

Para seleccionar destinos de informes

1. Abra el asistente de programación de alertas de acción, introduzca la información necesaria y vaya al paso de selección de servidores.
2. Seleccione los servidores disponibles que desea emplear para la consulta y desplácelos al área de servidores seleccionados mediante el control de cambio.
3. (Opcional) Si desea desactivar las consultas federadas de esta tarea de alerta, seleccione "No" en el menú desplegable que aparece cuando hace clic en la entrada de consultas federadas. Las consultas de informes se federan de forma predeterminada.
4. Vaya al paso de programación que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la tarea de alerta se programa; si no es así, aparece el paso que haya seleccionado.

Ejemplo: Crear una alerta de acción para el espacio en disco bajo

El espacio en disco disponible bajo es una de las consultas predefinidas mediante la etiqueta de alertas de acción. Las consultas de la etiqueta de alertas de acción se han diseñado especialmente para emplearse como alertas, pero no se convierten en alertas hasta que no se programan.

En el ejemplo siguiente, se indica cómo crear una alerta de acción de la consulta predefinida de espacio en disco bajo.

1. Haga clic en la ficha Consultas e informes y en la subficha Consultas.

Aparecen los paneles de etiqueta de consulta y de lista de consultas.

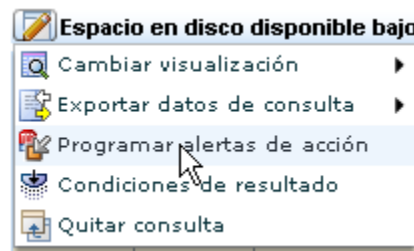
2. Haga clic en la etiqueta Alertas de acción.

La lista de consultas muestra las consultas etiquetadas como alertas de acción.

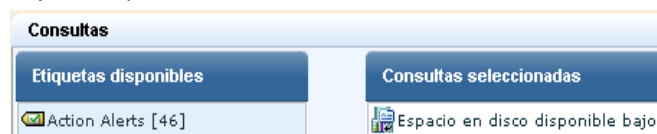
3. Haga clic en la consulta de espacio en disco disponible bajo de la lista de consultas.

La consulta de espacio en disco disponible bajo aparece en el panel principal.

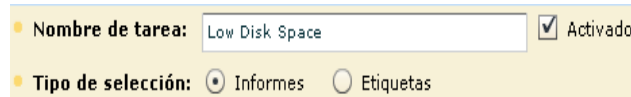
4. Haga clic en Opciones y seleccione Programar alertas de acción.



Aparece el asistente de programación de alertas de acción con el paso de selección de alertas seleccionado. La opción Espacio en disco disponible bajo está preseleccionada en Consultas seleccionadas.



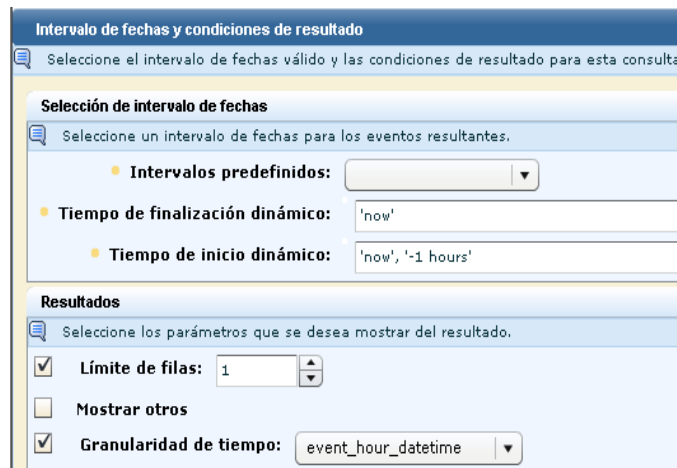
5. Introduzca un nombre de tarea, como Espacio en disco bajo. Por ahora, no seleccione la casilla de verificación Activado. Esto le permite guardar y cerrar la planificación de la alerta de acción antes de que esté finalizada sin arriesgarse a que se ejecute.



Nombre de tarea: ☒ Activado

Tipo de selección: ☒ Informes ☐ Etiquetas

6. Puede acceder o pasar por alto los filtros de alerta. Los filtros se añaden, es decir, cuando se evalúa una serie de filtros, éstos se unen mediante AND lógicos.
7. Haga clic en Condiciones de resultado para anular las establecidas en la definición de la consulta.
- Para especificar que la alerta debería evaluar el espacio en disco durante la hora anterior, establezca el rango de fechas como 'Ahora' para Hora de finalización dinámica y 'Ahora' '-1 hora' para Hora de inicio dinámica.
 - Para especificar que sólo desea recibir una notificación si la consulta obtiene resultados y que sólo quiere ver el primer resultado obtenido, seleccione Límite de filas y seleccione el valor 1. Como el rango de tiempo dinámico está establecido en horas, seleccione event_hour_datetime como granularidad de tiempo.
 - Deje los eventos agrupados en blanco, ya que eso no se aplica a esta consulta.



Intervalo de fechas y condiciones de resultado

Seleccione el intervalo de fechas válido y las condiciones de resultado para esta consulta.

Selección de intervalo de fechas

Seleccione un intervalo de fechas para los eventos resultantes.

Intervalos predefinidos:

Tiempo de finalización dinámico:

Tiempo de inicio dinámico:

Resultados

Seleccione los parámetros que se desea mostrar del resultado.

☒ Límite de filas:

☐ Mostrar otros

☒ Granularidad de tiempo:

8. Haga clic en Programar tareas para definir la programación. La opción predeterminada es iniciar la tarea de forma inmediata y sin fecha de finalización. Defina el intervalo de repetición. Por ejemplo, establezca el intervalo para que ejecute la consulta cada hora.

Definir la programación

Programe las alertas de acción para que empiecen y se detengan en la misma fecha y a la misma hora o programe cada alerta individualmente.

Intervalo de repetición: 1 Horas

9. Haga clic en el paso Destino. Active la notificación por correo electrónico e introduzca su dirección de correo electrónico en el campo Enviar correo a. También puede introducir un asunto y un cuerpo del mensaje. Asimismo, puede enviar un mensaje de correo electrónico a los destinatarios deseados e introducir su dirección de correo electrónico en el campo del remitente. Si introduce varias direcciones de correo electrónico, sepárelas mediante una coma (no utilice el punto y coma).

Correo electrónico

Seleccione la casilla de verificación para especificar la dirección de correo electrónico.

☒ **Activar notificación por correo electrónico**

Enviar correo a: username@company.com Desde: username@company.com

Asunto: Low Disk Space Notification

Texto de correo electrónico: Disk space has dropped bellow 20%.

10. Haga clic en Selección de servidor. De forma predeterminada, la consulta se ejecutará en el servidor de CA Enterprise Log Manager actual. Seleccione Federado para ejecutar la consulta en este servidor y todas las consultas federadas que se pueden seleccionar.
11. Haga clic en Selección de alertas. Seleccione Activado.
12. Haga clic en Guardar y cerrar.

Esta tarea de alerta de acción se muestra en la subficha Programación de alertas.

Tareas de alerta de acción								
Nombre de tarea	Activado	Servidor	Repetición	Fecha y hora de inicio	Hora de finalización	Zona horaria	Creador	
Low Disk Space	true	caelm5	1 hour	Mon Sep 28 2009 10:12:08 am		America/New_York	Administrator1	

13. Haga clic en Alertas de acción en la ficha Gestión de alertas para visualizar los resultados de esta alerta de acción.

Recibirá la notificación por correo electrónico solicitada. A continuación, se muestra un ejemplo:

Asunto: Low disk space Notification

CA Enterprise Log Manager	
RSS enlace	https://calmrhbuildtest01:5250/spin/calm/getAc8424346294223181834-calmrhbuildtest01122053207977576_actionquery_1220536215721
Nombre de consulta	Espacio en disco disponible bajo
Fecha generada	miércoles 21 de octubre de 2009 12H35' EDT
Etiquetas	[Action Alerts]
Creador	Administrator1
Servidor	caelm
Comentarios	
Disk space has dropped below 20%	

Si hace clic en el vínculo de RSS, aparece una página parecida a ésta:

CA ELM Alerta de Acción resultado de conjunto		
Título: Espacio en disco disponible bajo		
Creador: Administrator1		
Tiempo de ejecución: Martes, 08/12/09 16:35:46 EDT		
event_hour_datetime	receiver_hostname	dest_objectvalue

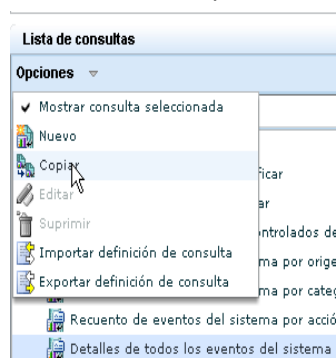
Ejemplo: Crear una alerta para un evento autocontrolado

La consulta predefinida para todos los eventos autocontrolados es Detalles de todos los eventos del sistema. Puede copiar esta consulta y emplearla como base para la definición de una alerta basada en un evento autocontrolado determinado.

Por ejemplo, se genera un evento autocontrolado cuando, en una actualización de suscripción, se carga un módulo que requiere que reinicie el sistema operativo. Este evento autocontrolado sólo se genera una vez. Puede que desee crear una alerta como recordatorio para reiniciar el sistema operativo en el caso de que este evento de autocontrol se pase por alto.

Utilice el ejemplo siguiente como guía.

1. Cree una consulta basada en la consulta para todos los eventos autocontrolados tal y como se indica a continuación:
 - a. Haga clic en la ficha Consultas e informes y en la subficha Consultas.
 - b. Seleccione Detalles de todos los eventos del sistema en la lista de consultas, expanda la lista desplegable Opciones y seleccione Copiar.



Aparece el asistente de diseño de consulta con el paso de detalles seleccionado.

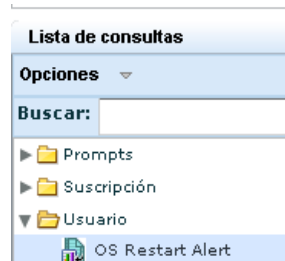
- c. Sustituya el nombre de la consulta copiada por un nombre nuevo, por ejemplo, Alerta de reinicio del SO. También puede añadir un nombre corto y una descripción nueva.
 - d. Seleccione Alertas de acción en Etiquetas disponibles y desplácelo a Etiquetas seleccionadas.

2. Cree filtros de consultas del modo que se indica a continuación:
 - a. Vaya al paso de filtros de consulta. Haga clic en la ficha Filtros avanzados.
 - b. Haga clic en Nuevo filtro de evento. Seleccione event_logname como columna, deje Equal to como operador y seleccione CALM como valor.
 - c. Haga clic en Nuevo filtro de evento. Seleccione receiver_name como columna, deje Equal to como operador e introduzca Suscripción.
 - d. Haga clic en Nuevo filtro de evento. Seleccione result_string como columna, deje Equal to como operador e introduzca el mensaje: Se han instalado actualizaciones del SO en este host... Reinicie el equipo para que las actualizaciones surtan efecto.

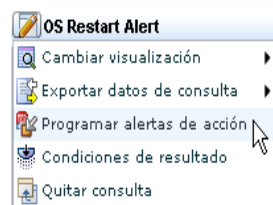
Filtros avanzados				
Para filtrar los eventos, defina una sentencia condicional en el control de filtros.				
	(			)
Lógica	(	Columna	Operador	Valor
	(	event_logname	Igual a	CALM
And		receiver_name	Igual a	Subscription
And		result_string	Igual a	OS Updates are installed on this host...Please restart the machine for these updates to have effect !!!

3. Haga clic en Guardar y cerrar.

La alerta nueva aparece en la lista de consultas de la carpeta Usuario.



4. Programe una alerta de acción para la consulta definida por el usuario según los pasos que se indican a continuación:
 - a. Seleccione la consulta en la carpeta Usuario.
 - b. Haga clic en el botón Editar del panel derecho para mostrar la lista desplegable de alerta de reinicio del SO y seleccione Programar alertas de acción de acción.



Aparece el asistente de programación de alertas de acción y muestra el paso de selección de alertas. La alerta de reinicio del SO está preseleccionada en las consultas seleccionadas.

- c. Introduzca un nombre de tarea. Por ejemplo, introduzca Alerta de reinicio del sistema operativo.

5. Agregue un filtro de eventos del modo siguiente:

- a. Haga clic en Filtros de alerta.
- b. Haga clic en Nuevo filtro de evento.
- c. Seleccione receiver_hostname como columna, deje Equal to como operador e introduzca el nombre del CA Enterprise Log Manager local como valor.

Filtros avanzados				
Para filtrar los eventos, defina una sentencia condicional en el control de filtros.				
Lógica	(	Columna	Operador	Valor
		receiver_hostname	Igual a	LogManager02
	)			

6. Especifique la frecuencia con la que desea generar la alerta cuando sea necesario reiniciar el sistema del modo siguiente:
 - a. Haga clic en Programar tareas.
 - b. Establezca el intervalo de repetición para la frecuencia de generación de la alerta. Por ejemplo, seleccione 1 y Días para generarla una vez al día.
7. Indique los datos de correo electrónico como se indica a continuación para recibir la alerta por correo electrónico.
 - a. Haga clic en el paso Destino.
 - b. Haga clic en Activar notificación por correo electrónico e introduzca la dirección de correo electrónico y otros datos opcionales si lo desea.
8. Restrinja la notificación a los casos en los que el servidor actual deba reiniciarse del modo siguiente:
 - a. Haga clic en Selección de servidor.
 - b. Seleccione No en la opción Consulta federada.

9. Haga clic en Guardar y cerrar para guardar la tarea de alerta.

La tarea de alerta de acción aparece en la ficha Gestión de alertas, en la subficha Programación de alertas.

Tareas de alerta de acción					
Nombre de tarea ▼	Activado	Servidor	Repetición	Fecha y hora de inicio	Hora de finalización
Restart Operating System Alert	verdadero	caelm5	1 día	Viernes, 30/10/09 16:12:19	

Ejemplo: Envío de un correo electrónico al Administrator cuando se detiene el flujo de eventos

Es necesario notificar a los administradores cuando un conector de un agente deja de recopilar eventos. Puede automatizar esta notificación cuando un indicador sugiere que se ha producido. Puede configurar el indicador, que es el tiempo que transcurre desde que un servidor de recopilación recibió los eventos desde cualquier conector. El tiempo transcurrido se puede configurar como el número que desee de minutos, horas o días. Esta consulta se puede extender a todos los servidores de recopilación de la federación.

Para limitar el número de mensajes de correo electrónico que se envía cuando un conector deja de funcionar, tenga en cuenta sólo aquellos conectores que hayan recopilado eventos hasta ahora. Por ejemplo, configure la alerta para que sólo devuelva filas de los conectores que hayan recopilado eventos durante la hora anterior a la actual pero no hayan recopilado eventos durante la última hora.

Para capturar estos datos, seleccione la consulta predefinida, Controlador de recopilación por gestor de registros: Desactivación del conector de agente. Esta consulta devuelve el nombre del conector y del agente cuando no se reciben eventos de acuerdo con lo definido en Condiciones de resultado en la alerta. Utilice los ejemplos siguientes como guía para generar una alerta cuando no se reciban eventos durante la última hora desde un conector que haya enviado eventos durante el período comprendido entre una y dos horas previas a la actual. Para el destino de alerta, especifique la dirección de correo electrónico de la persona a la que se vaya a enviar la notificación. Para que la programación ejecute una consulta, especifique una frecuencia mayor o igual a la del periodo de tiempo transcurrido.

Nota: La configuración del correo electrónico se debe definir en Administración, Servidor de informes, antes de crear la alerta.

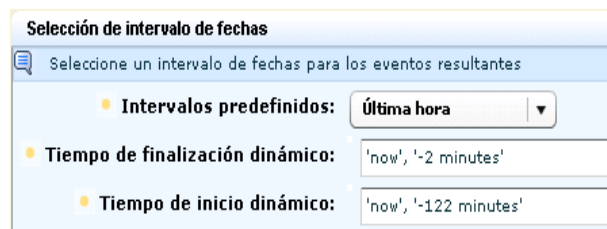
Para enviar un correo electrónico al administrador cuando un conector deja de recopilar eventos

1. Seleccione el servidor desde el que desee ejecutar esta alerta. En una arquitectura de concentrador y periferia, seleccione un servidor de recopilación para que capture la condición lo antes posible.
2. Seleccione la ficha Gestión de alertas y en la subficha Programación de alertas.
3. Haga clic en Programar una alerta de acción.
4. Introduzca el nombre de la tarea, por ejemplo, Conector fuera de servicio.
5. En Consultas disponibles, seleccione Controlador de recopilación por gestor de registros: Desactivación del conector de agente y desplácese hasta la lista Consultas seleccionadas.



6. Haga clic en Condiciones de resultado.
7. Configure el tiempo durante las dos últimas horas.
 - a. Seleccione los intervalos predefinidos Última hora.

De este modo, la hora de finalización dinámica se establecerá correctamente como 'ahora, '-2 minutos'.
 - b. Haga clic en Editar cadena para el tiempo dinámico para el tiempo de inicio dinámico.
 - c. En Cadena para tiempo dinámico, sustituya 62 por 122.
 - d. Haga clic en Aceptar.



8. Configure las condiciones de resultado.

- a. Seleccione Últimos eventos agrupados con fecha anterior y haga clic en Editar.
- b. Seleccione Ahora para el tiempo de referencia y haga clic en Agregar hora de referencia a la cadena de tiempo dinámica.
- c. Haga una vez en el control de hora del turno para mostrar -1, seleccione hora en la lista desplegable y haga clic en Agregar hora del turno a la cadena para el tiempo dinámico.
- d. Haga clic en Aceptar.



9. Haga clic en el paso Programar tareas y define el intervalo de repetición. Por ejemplo, configure el intervalo en una hora.



10. Haga clic en Destino y complete la ficha Correo electrónico.

- a. Seleccione Activar notificación por correo electrónico.
- b. Introduzca la dirección de correo electrónico para Enviar correo a.
- c. Introduzca la dirección de correo electrónico para Correo electrónico de.
- d. Escriba el asunto en el campo Asunto. Por ejemplo, escriba "El conector puede estar fuera de servicio".
- e. Introduzca el texto del correo electrónico. Por ejemplo, escriba: El conector ha dejado de enviar eventos durante la última hora.

11. Haga clic en el paso Selección de servidor y borre Federado, si lo desea.
12. Haga clic en Guardar y cerrar.

Puede definir esta alerta para que consulte el intervalo de fechas en días, en lugar de hacerlo en horas y, a continuación, programarla para que se ejecute una vez al día. En este caso, el tiempo de finalización dinámico se configuraría como 'ahora', el tiempo de inicio dinámico se configuraría como 'ahora', '-2 días' y el último evento agrupado con fecha anterior se configuraría como 'ahora', '-1 días'.

Configuración de retenciones de alertas de acción

Puede controlar la cantidad de alertas de acción que se guardarán en el servidor de informes, así como el tiempo durante el que se retendrán.

Para configurar retenciones de alertas de acción

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
Aparece la lista de servicios.
2. Haga clic en el servidor de informes para la configuración global, o en el host del servidor de informes para la configuración local.
Aparece el panel de configuración del servidor de informes.
3. Introduzca un valor en el campo de entrada Número máximo de alertas de acción. Cualquier alerta que supere ese límite se eliminará, comenzando por las más antiguas.
4. Introduzca un número de días en el campo de entrada Retención de alertas de acción. Cuando transcurran esos días, las alertas se eliminarán.
Nota: Las alertas de acción se eliminan cuando se supera uno de los límites.
5. Haga clic en Guardar.

Ejemplo: Crear una alerta para Business_Critical_Sources

Puede crear una consulta personalizada con la lista con clave Business_Critical_Sources y programar una alerta basada en esta consulta. La lista con clave es aquella que no contiene valores predeterminados y no cuenta con alertas o consultas predefinidas asociadas. Utilice el siguiente proceso completo como guía.

1. Instale un agente.
2. Configure un conector en dicho agente para recopilar eventos de cada origen crítico para el negocio.

Detalles del estado	
Reiniciar	Iniciar
Detener	
Conector	Agente
NTEventLog_Connector	USER001LAB.ca.com

3. Defina los valores de nombre de host de las listas definidas por el usuario (claves) de Business_Critical_Sources.
 - a. Haga clic en la ficha Administración y en la subficha Servicios.
 - b. Seleccione Servidor de informes en la lista de servicios.
 - c. Seleccione Business_Critical_Sources en el área de listas definidas por el usuario (claves).
 - d. Haga clic en Agregar valor en el área de valores e introduzca el nombre de host de un origen crítico para el negocio.

Valores de clave	Valores
Privileged_Groups	USER001LAB
Business_Critical_Sources	

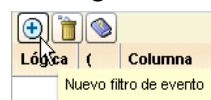
- e. Repita el último paso para cada origen crítico para el negocio del que se recopilan eventos.
- f. Haga clic en Guardar.

4. Cree una consulta sobre los intentos de inicio de sesión erróneos en orígenes críticos para el negocio.
 - a. Haga clic en Consultas e informes.
 - b. En la lista de consultas, escriba inicio de sesión en el campo de búsqueda.
 - c. Seleccione Intentos de inicio de sesión incorrectos por host y seleccione Copiar en la lista desplegable Opciones.

Se abre el asistente de diseño de consulta con el nombre Copia de Intentos de inicio de sesión incorrectos por host.

Cambie el nombre de la consulta por Intentos de inicio de sesión incorrectos por Business_Critical_Sources.

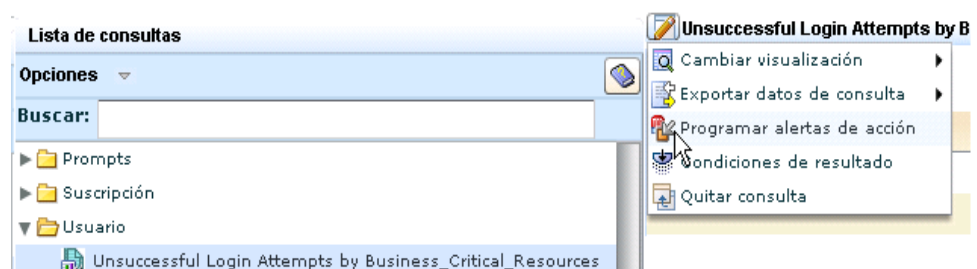
- d. Seleccione el paso de filtros de consulta.
- e. Haga clic en la ficha Filtros avanzados.
- f. Haga clic en Nuevo filtro de evento.



- g. Seleccione source_hostname como columna, seleccione Keyed como operador y seleccione Business_Critical_Sources como valor.

Lógica	(	Columna	Operador	Valor	)
		source_hostname	Con clave	Business_Critical_Sources	

- h. Haga clic en Guardar y cerrar.
5. Planifique una alerta basada en esta consulta personalizada.
 - a. Haga clic en la ficha Consultas e informes.
 - b. Seleccione Intentos de inicio de sesión incorrectos por Business_Critical_Sources en la carpeta Usuario de la lista de consultas.
 - c. Seleccione Programar alertas de acción en la lista desplegable Editar.



Aparece el asistente de programación de alertas de acción.

- d. Introduzca el nombre de una tarea, como Intentos de inicio de sesión incorrectos por Business_Critical_Sources
 - e. Haga clic en Programar tareas y defina la programación.
 - f. También puede especificar las opciones de correo electrónico del destino.
 - g. Haga clic en Guardar y cerrar.
6. Compruebe que la tarea está programada.
- a. Haga clic en la ficha Gestión de alertas y en la subficha Programación de alertas.
 - b. Compruebe que aparece el nombre de la tarea introducida.

Tareas de alerta de acción	
Nombre de tarea ▼	Activado
Unsuccessful Login Attempts by Business Critical Resources	verdadero

7. Compruebe que la alerta se genera.
- a. Haga clic en la ficha Gestión de alertas. Aparece la subficha Alertas de acción.
 - b. Visualice las alertas que se muestran para determinar si aparece el nombre de la tarea incluida.

Edición de alertas de acciones

Puede editar alertas de acciones existentes.

Para editar alertas de acciones

1. Haga clic en la ficha Gestión de alertas.
Aparece la lista de servidores de alertas.
2. Seleccione el servidor en el que se ha programado la alerta de acción que desea editar.
Aparece el panel de detalles del servidor, en el que se muestra la ficha Informes generados de forma predeterminada.
3. Haga clic en la ficha Alertas programadas, seleccione la alerta deseada y haga clic en Editar en la parte superior de la lista.
Aparece el asistente de programación de alertas de acción.
4. Realice los cambios deseados y haga clic en Guardar y cerrar.
La alerta de acción editada aparece en la lista de alertas de acción.

Activación o desactivación de alertas de acción

Puede desactivar una o varias alertas de acción cuando ya no desee que se ejecuten las consultas programadas asociadas a esa alerta de acción. Se pueden activar alertas de acción que se desactivaron anteriormente, de manera que se puedan ejecutar de acuerdo con la programación guardada.

Para activar o desactivar las tareas de alertas de acción

1. Haga clic en la ficha Gestión de alertas y en la subficha Programación de alertas.

Aparecerá la lista Alertas de acción que mostrará el estado de cada tarea en la columna Activado. Si la tarea está activada, se aplicará el valor Activado. Si está desactivada, no se aplicará el valor Activado.

2. Seleccione la tarea o las tareas que desee y haga clic en Activar seleccionados o Desactivar seleccionados.

La lista Tareas de alerta de acción mostrará el nuevo estado de todas las tareas que haya activado o desactivado.

Nota: La capacidad para desactivar tareas de alerta está diseñada para usarla con alertas repetidas. Si desactiva una tarea de alerta con una sola aparición ("Una vez"), se eliminará de la lista Tareas de alerta de acción.

Eliminación de alertas de acciones

Puede eliminar alertas de acciones no necesarias.

Para eliminar alertas de acciones

1. Haga clic en la ficha Gestión de alertas.
Aparece la lista de servidores de alertas.
2. Seleccione el servidor que contiene la alerta de acción que desea eliminar.
Aparece el panel de detalles del servidor.
3. Haga clic en la ficha Alertas programadas, haga clic en la fila para seleccionar la alerta deseada y haga clic en Suprimir en la parte superior de la lista. Puede seleccionar varias tareas de alerta para suprimirlas.

Nota: Las casillas de verificación que se encuentran junto a cada tarea de alerta permiten activar o desactivar tareas de alerta.

Aparecerá un cuadro de diálogo de confirmación.

4. Haga clic en Sí.
Aparece un mensaje que indica que la eliminación se ha realizado correctamente.
5. Haga clic en Aceptar.
La tarea de alerta se elimina de la lista de tareas de alerta.

Capítulo 13: Informes programados

Esta sección contiene los siguientes temas:

[Visualización de informes generados](#) (en la página 503)
[Anotación de informes generados](#) (en la página 505)
[Programación de tareas de informes](#) (en la página 506)
[Ejemplo: Programar informes con una etiqueta común](#) (en la página 517)
[Ejemplo: Enviar por correo electrónico de forma diaria informes de PCI en formato PDF](#) (en la página 521)
[Edición de tareas de informes programadas](#) (en la página 522)
[Activación y desactivación de tareas de informes programados](#) (en la página 523)
[Eliminación de tareas de informes programadas](#) (en la página 524)
[Eventos autocontrolados](#) (en la página 524)
[Visualización de eventos autocontrolados](#) (en la página 525)

Visualización de informes generados

Puede visualizar un informe generado o guardar una copia en la ubicación que seleccione. Los informes generados se almacenan en el dispositivo informático con CA Enterprise Log Manager en la siguiente ruta:

/opt/CA/LogManager/data/reports

Para ver informes generados

1. Haga clic en la ficha Informes programados.
La ficha se abre y muestra el host de CA Enterprise Log Manager local de forma predeterminada.
2. Seleccione el servidor donde se han programado los informes generados que desea ver.
El servidor que seleccione se mostrará en el panel de detalles.
3. Haga clic en la ficha Informes generados si aún no se muestra.
Aparece la lista de informes generados.
4. Haga clic en el nombre del informe que desee visualizar.
Aparecerá el cuadro de diálogo Guardar.
5. Haga clic en Guardar para definir una ubicación en la que guardar el informe.

Más información:

[Filtrado de informes](#) (en la página 504)

[Anotación de informes generados](#) (en la página 505)

[Programación de tareas de informes](#) (en la página 506)

[Eventos autocontrolados](#) (en la página 524)

Filtrado de informes

Puede definir filtros para refinar la visualización de las tareas de informes programadas y de los informes generados disponibles.

Para filtrar informes generados o programados

1. Seleccione el servidor de informes en el que se encuentran los informes programados o generados que desea filtrar y haga clic en la ficha Informes generados o Informes programados.

Aparece la lista de informes generados o informes programados.

2. Seleccione el tipo de repetición o formato por el que desea filtrar los informes visualizados mediante los menús desplegables correspondientes.

La lista muestra los informes que cumplen los requisitos del filtro.

Más información

[Visualización de informes generados](#) (en la página 503)

[Anotación de informes generados](#) (en la página 505)

Anotación de informes generados

Puede agregar anotaciones a un informe generado con el fin de realizar revisiones o un seguimiento de dicho informe.

Para anotar informes generados

1. Seleccione el servidor de informes en el que se encuentran los informes generados que desea anotar y haga clic en la ficha Informes generados.

Aparece la lista de informes generados.

2. Haga clic en el icono de anotaciones situado junto al informe que desea anotar.

Aparece el cuadro de diálogo Anotaciones de informe, que muestra las anotaciones previas con el nombre de quien las creó, así como la fecha y la hora de la creación.

3. Introduzca la anotación deseada y haga clic en Guardar.

La anotación aparece en el cuadro de diálogo, que permanece abierto para permitirle realizar más anotaciones.

4. (Opcional) Repita el paso 3 para agregar más anotaciones.

5. Haga clic en Cerrar cuando no desee agregar más anotaciones.

El cuadro de diálogo Anotaciones de informe se cierra.

Más información

[Visualización de informes generados](#) (en la página 503)

[Filtrado de informes](#) (en la página 504)

Programación de tareas de informes

El proceso de creación de tareas de informes mediante el asistente de programación de informes consta de los siguientes pasos principales:

1. Apertura del asistente de programación de informes.
2. Selección de plantillas de informe: para comenzar a programar una tarea de informes, debe seleccionar el informe o la etiqueta que desea emplear como plantilla para la tarea. Puede seleccionar una única plantilla o etiqueta, o bien múltiples plantillas o etiquetas.
3. Creación de filtros de informe: si lo necesita, puede aplicar filtros de eventos avanzados para personalizar aún más los resultados de los informes.
4. Establecimiento del intervalo de fechas y las condiciones del resultado: puede establecer el intervalo de fechas durante el que desea que la consulta del informe realice búsquedas y otras condiciones.
5. Programación de tareas: debe establecer el día y la hora en que se ejecutan los informes tanto en casos únicos como en informes repetidos. También puede seleccionar uno de los patrones de repetición disponibles.
6. Selección de destino y formato del informe: puede seleccionar el formato de informe que desee, así como las opciones de envío de mensajes de correo electrónico.
7. Selección de un servidor: debe seleccionar el servidor al que realizará consultas el informe y si también se consultará a los hosts federados del servidor.

Apertura del asistente de programación de informes

Para crear una tarea de informe nueva para uno o varios informes que se repiten, debe emplear el asistente de programación de informes.

Para abrir el asistente de programación de informes

1. Haga clic en la ficha Informes programados.
Aparece la lista de servidores de informes.
2. Seleccione el servidor en el que desea programar un informe.
El panel Detalles del servidor de informes muestra el servidor seleccionado, en el que aparece la ficha Informes generados de forma predeterminada.
3. Haga clic en la ficha Programación de informes y, a continuación, haga clic en Programar un informe.

Aparece el asistente de programación de informes.

Al emplear el asistente:

- Haga clic en Guardar y Cerrar para guardar el informe programado y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Más información

[Establecimiento de parámetros de programación](#) (en la página 515)

[Creación de filtros de eventos avanzados](#) (en la página 597)

[Configuración de condiciones del resultado](#) (en la página 511)

[Selección de un objetivo de consulta de informe](#) (en la página 517)

Selección de plantillas de informes

El primer paso para crear una tarea de informe es seleccionar la plantilla de informe. Si desea programar múltiples tareas de informes que compartan los mismos filtros, programación y configuración de destino, puede hacerlo seleccionando varios informes o etiquetas como plantillas.

Si selecciona varios informes, las tareas se mostrarán de forma separada para cada informe. Por ejemplo, si selecciona dos informes independientes, estos comparten la misma programación y las mismas opciones de filtro, pero se muestran de forma separada (por nombre de informe) en la lista Informes generados.

Los usuarios que tengan con el rol Administrator pueden crear tareas de informes en estado desactivado para utilizarlas posteriormente. Los usuarios con los roles Administrator y Analyst podrán activar y desactivar las tareas más adelante. Los informes desactivados mostrarán el valor *falso* en la columna Activado al visualizar la ficha Informes programados.

Para seleccionar plantillas de informes

1. Introduzca un nombre de tarea.
2. Seleccione la zona horaria en la que desea programar el informe en el menú desplegable de zonas horarias.
3. Seleccione el botón de opción Informes o Etiquetas para seleccionar los informes por etiqueta o de forma individual.

Nota: La programación de informes por etiquetas le permite agregar informes sin cambiar la tarea. Si selecciona la etiqueta Gestión de identidades, todos los informes que tengan esa etiqueta se añadirán a la tarea en el tiempo de ejecución programado. Esta función también se aplica a etiquetas personalizadas.

4. (Opcional) Seleccione una o varias etiquetas para limitar las etiquetas e informes individuales mostrados. Esta función coincide con el comportamiento de la lista de informes.
5. (Opcional) Anule la selección de la casilla de verificación Activado para crear la tarea de informe en estado desactivado. La casilla de verificación Activado se encuentra seleccionada de forma predeterminada.

Nota: La capacidad para crear una tarea de informe en estado desactivado está prevista para el uso con informes repetidos. Si anula la selección de la casilla de verificación Activado correspondiente a una tarea y crea la tarea con una sola repetición (Ahora o Una vez), dicha tarea se eliminará de la lista de informes programados.

6. (Opcional) Seleccione la casilla de verificación Conservar tras la caducidad para conservar la configuración del informe tras la generación del mismo.

Nota: Una vez generado el informe, es posible editar la plantilla del informe y reprogramar el mismo.

7. Seleccione las etiquetas o los informes individuales que desea emplear como plantillas de informe y utilice el control de cambio para agregarlos al área de informes seleccionados.
8. Vaya al paso de programación que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el informe se programa; si no es así, aparece el paso que haya seleccionado.

Uso de filtros avanzados

Puede usar filtros avanzados basados en SQL para calificar cualquier función que consulte el almacenamiento de registro de eventos, incluida la limitación de consultas o la personalización de filtros rápidos. La interfaz Filtros avanzados le ayuda a crear la sintaxis apropiada para los filtros proporcionando un formulario para introducir columnas, operadores y valores lógicos en función de los requisitos de filtrado.

Nota: Esta sección contienen una breve descripción general de los términos SQL usados en los filtros avanzados. Para aprovechar al máximo el potencial de los filtros avanzados, debe conocer a fondo SQL y la gramática de eventos comunes.

Los siguientes términos SQL unen varias instrucciones de filtros:

And

Muestra la información del evento si *todos* los términos unidos son verdaderos.

Or

Muestra la información del evento si *alguno* de los términos unidos es verdadero.

Having

Restringe las condiciones de la instrucción SQL principal añadiendo una instrucción de calificación. Por ejemplo, puede definir un filtro avanzado para eventos de determinados hosts y añadir una instrucción "having" para mostrar sólo los eventos de esos host que presenten un nivel de severidad específico.

Los filtros avanzados utilizan los siguientes operadores SQL para crear las condiciones básicas:

Operadores relacionales

Incluye la información del evento si la columna tiene la relación apropiada con el valor introducido. Dispone de los siguientes operadores relacionales:

- Equal to
- Not Equal to
- Less than
- Greater than
- Less than or equal to
- Greater than or equal to

Por ejemplo, si usa *Greater than*, incluiría la información del evento de la columna elegida si su valor fuera mayor que el valor especificado.

Like

Incluye la información del evento si la columna contiene un patrón que haya introducido, usando % para definir el patrón deseado. Por ejemplo, L% devolvería cualquier valor que empezara por L, y %L% devolvería cualquier valor que tuviera una L, pero no como primera o última letra.

Not like

Incluye la información del evento si la columna no contiene el patrón especificado.

In set

Incluye la información del evento si la columna contiene uno o varios valores del conjunto entrecomillado introducido. Debe separar con comas los diferentes valores del conjunto.

Not in set

Incluye la información del evento si la columna no contiene uno o varios valores del conjunto entrecomillado introducido. Debe separar con comas los diferentes valores del conjunto.

Matches

Incluye cualquier información del evento que coincida con uno o más de los caracteres introducidos, de manera que puede buscar por palabras clave.

Keyed

Incluye cualquier información del evento que se haya definido como valor clave durante la configuración del servidor de informes. Puede emplear valores clave para definir la relevancia empresarial u otros grupos organizativos.

Not Keyed

Incluye cualquier información del evento que no se haya definido como valor clave durante la configuración del servidor de informes. Puede emplear valores clave para definir la relevancia empresarial u otros grupos organizativos.

Configuración de condiciones del resultado

Puede configurar un intervalo de fechas y otras condiciones del resultado para la consulta, incluidos límites de filas y período de tiempo de base de visualización. Las condiciones del resultado se pueden modificar en cualquier momento hasta la hora de ejecución de la consulta, de manera que resultan un método útil para modificar consultas sin cambiar la consulta de base o sus filtros.

Puede establecer los tipos de condiciones del resultado siguientes:

- Condiciones de intervalo de fechas que controlan el período de búsqueda de la consulta
- Condiciones de visualización, como el número máximo de filas
- Condiciones de eventos agrupados, como los eventos agrupados más recientes tras una fecha determinada o los eventos agrupados que contienen un cierto número de eventos

Nota: Si no agrupa al menos una columna al crear la consulta, los usuarios no podrán editar las condiciones del resultado en la pantalla de consultas.

Establecimiento de intervalos de fecha y hora

Puede establecer una condición de intervalo de fecha y hora para su consulta. Esto mejora la eficacia de la consulta reduciendo la parte del almacenamiento del registro de eventos que debe buscar.

Puede utilizar un intervalo de tiempo predefinido, o bien crear uno personalizado. Para que el intervalo de tiempo personalizado funcione correctamente, debe establecer tanto una hora de inicio como de finalización. Si sólo establece un parámetro de hora, se expresa como una cláusula "Where" en SQL de consulta.

Para configurar condiciones de resultado

1. Abra el cuadro de diálogo de condiciones de resultados.
2. Seleccione un intervalo de tiempo predefinido en la lista desplegable. Por ejemplo, si desea ver los eventos recibidos el día anterior, seleccione "Día anterior".

Nota: Si está creando una alerta de acción o un informe programado, la interfaz muestra los siguientes intervalos de hora predeterminados.

- Alerta de acción: los 5 minutos anteriores
- Informe programado: las 6 horas anteriores

3. (Opcional) Cree un intervalo de tiempo personalizado con los pasos secundarios siguientes:
 - a. Haga clic en Editar junto al campo de entrada "Tiempo de finalización dinámico" en el área Selección del intervalo de fechas. Esto le permite establecer la finalización del período que desee que busque la consulta.
Aparece el cuadro de diálogo Especificación de tiempo dinámico.
 - b. Seleccione el tiempo de referencia que servirá de base para el parámetro y haga clic en Agregar.
 - c. Seleccione el parámetro de hora que desee y haga clic en Agregar. Puede agregar varios parámetros de hora.
 - d. Cuando haya terminado de agregar parámetros, haga clic en Aceptar.
El cuadro de diálogo Especificación de tiempo dinámico se cierra y los valores que seleccione aparece en el área "Tiempo de finalización dinámico". Si usa varios parámetros, éstos forman una instrucción de hora completa y cada parámetro hace referencia al primero. Por ejemplo, si agrega "Inicio del mes" y "Día de la semana: martes", los valores en el área "Hora de finalización dinámica" finalizará la consulta el primer martes del mes.

Nota: si usa "Numero de" valores, como "Número de días" o "Número de horas", debe introducir un número *negativo* para establecer una hora pasada. Si utiliza un número positivo se establecerá una hora de finalización futura y provocará que la consulta continúe enviando resultados siempre que al menos un evento categorizado se encuentre en el almacén de registros.

Por ejemplo, si agrega los valores "ahora" y "número de minutos: 10" al área "Hora de inicio dinámica" inicia la consulta 10 minutos antes de la hora de finalización seleccionada.

- e. Repita el paso 2 en el área "Hora de inicio dinámica" para establecer el principio del período que desee que busque la consulta.

Si no introduce un intervalo de fecha, la consulta se aplica a todos los eventos en el almacén de registros.

4. Haga clic en la flecha correspondiente para avanzar al paso de diseño de consulta que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la consulta nueva aparece en la lista de consultas; si no es así, aparece el paso de diseño de consulta que haya seleccionado.

Más información

[Configuración de condiciones del resultado](#) (en la página 511)

[Establecimiento de condiciones de grupo y visualización](#) (en la página 514)

Establecimiento de condiciones de grupo y visualización

Puede establecer condiciones que permitan el control de las condiciones y visualización de consultas que busquen eventos basados en cómo se han agrupado.

Para establecer condiciones de grupo y visualización

1. Abra el cuadro de diálogo de condiciones de resultados.
2. Use los cuadros de diálogo Resultados para activar uno de las siguientes categorías de visualización que desee:

Límite de filas

Establece el número máximo de filas de eventos que muestra la consulta. Se comienza por los eventos más recientes.

Mínimo: 1

Máximo: 5000

Mostrar otros

Indica la presencia de otros resultados que no se muestran debido al límite de filas, lo que le permite comparar los eventos seleccionados en el contexto de todos los eventos de ese tipo. Por ejemplo, si selecciona un límite de fila de 10 para la visualización del visor de eventos y selecciona que se muestren otros, los eventos superiores a 10 se muestran como una única entrada titulada Otros, que muestra los eventos restantes. Esta configuración sólo es efectiva cuando se selecciona el límite de filas.

Granularidad de tiempo

Establece el nivel de detalles del campo de período de tiempo utilizado en la pantalla de consulta.

3. Utilice Condiciones del resultado para consultar varios tipos o condiciones de eventos agrupados. Por ejemplo, podría establecer su consulta para buscar el último evento agrupado después de una fecha seleccionada o un número determinados de eventos de grupo. Un evento agrupado es un evento refinado para el que ha establecido una función y orden de grupo en el paso de creación de consulta.

Las condiciones de grupo utilizan el mismo sistema de instrucción de hora que los campos de intervalos de hora.

4. Haga clic en la flecha correspondiente para avanzar al paso de diseño de consulta que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la consulta nueva aparece en la lista de consultas; si no es así, aparece el paso de diseño de consulta que haya seleccionado.

Más información

[Configuración de condiciones del resultado](#) (en la página 511)

Establecimiento de parámetros de programación

Puede controlar cuándo se ejecutan los informes programados, si desea que se repitan, así como el intervalo de repetición.

Para establecer parámetros de programación

1. Abra el asistente de programación de informes y vaya al paso de programación de tareas.
2. Utilice los botones de opción Sin repetición o Repetición para seleccionar la hora de la generación del informe y el patrón de repetición deseado, en caso de que lo establezca.

Nota: Si emplea el horario de verano en su entorno, no programe un informe durante el tiempo de cambio, ya que no se generará. Por ejemplo, si el horario de verano comienza a las 2:00 h del 8 de marzo, no puede programar un informe entre las 2:00:00 h y las 2:59:59 h.

3. Vaya al paso de programación que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el informe se programa; si no es así, aparece el paso que haya seleccionado.

Más información

[Uso de filtros avanzados](#) (en la página 509)

[Configuración de condiciones del resultado](#) (en la página 511)

[Selección de un objetivo de consulta de informe](#) (en la página 517)

Selección de ajustes de formato y notificación

Puede seleccionar si los informes se generan en formato PDF, Excel o XML. También puede establecer una notificación automática mediante correo electrónico.

Para establecer el formato y la notificación

1. Abra el asistente de programación de informes y vaya al paso de destino.
2. Seleccione el formato deseado en el menú desplegable Formato de informe.

Nota: En el formato PDF, los gráficos se limitan a un máximo de 100 puntos de datos, lo que permite leer con claridad los rótulos de los ejes. Si el gráfico que desea visualizar contiene más de 100 puntos, CA Enterprise Log Manager incluirá únicamente los primeros 100 puntos en el resultado publicado en PDF.

3. Seleccione la casilla de verificación de correo electrónico si desea enviar una notificación cuando se haya generado el informe.

Aparecen los campos de especificación del correo electrónico.

4. Introduzca las direcciones de correo electrónico de los usuarios que desea que reciban la notificación. Separe las direcciones mediante comas.
5. (Opcional) Introduzca otras especificaciones deseadas, como el asunto, la dirección de respuesta y el cuerpo del mensaje.
6. (Opcional) Seleccione Adjuntar informe para adjuntar al correo electrónico de notificación una copia del informe en el formato seleccionado.
7. Vaya al paso de programación que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el informe se programa; si no es así, aparece el paso que haya seleccionado.

Más información:

[Uso de filtros avanzados](#) (en la página 509)

[Configuración de condiciones del resultado](#) (en la página 511)

[Establecimiento de parámetros de programación](#) (en la página 515)

[Selección de un objetivo de consulta de informe](#) (en la página 517)

Selección de un objetivo de consulta de informe

Puede seleccionar qué sistema de almacenamiento de registro de evento federado busca la consulta de informe.

Para seleccionar destinos de informes

1. Abra el asistente de programación de informes y vaya al paso de selección de servidor.
2. Seleccione los servidores disponibles que desea emplear para la consulta y desplácelos al área de servidores seleccionados mediante el control de cambio.
3. (Opcional) Si desea desactivar las consultas federadas de este informe, seleccione "No" en el menú desplegable que aparece cuando hace clic en la entrada de consultas federadas. Las consultas de informes se federan de forma predeterminada.
4. Vaya al paso de programación que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el informe se programa; si no es así, aparece el paso que haya seleccionado.

Más información

[Uso de filtros avanzados](#) (en la página 509)

[Configuración de condiciones del resultado](#) (en la página 511)

[Establecimiento de parámetros de programación](#) (en la página 515)

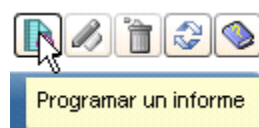
Ejemplo: Programar informes con una etiqueta común

Puede programar uno o varios informes para que se generen con una frecuencia determinada con una fecha de finalización específica.

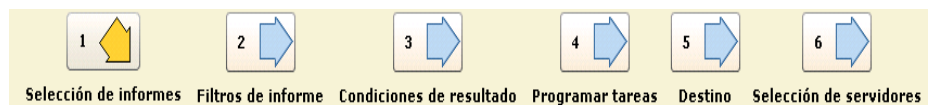
Los auditores, los analistas y los administradores pueden programar informes.

Para programar un informe

1. Haga clic en la ficha Informes programados, en la subficha Programación de informes y, a continuación, haga clic en Programar un informe.



Aparece el asistente de programación de informes con el paso 1, Seleccionar informe, seleccionado.



2. Introduzca el nombre de una tarea, seleccione Informes para habilitar la selección de informes individuales o seleccione Etiquetas para habilitar la selección de todos los informes asociados a una etiqueta seleccionada.

En el ejemplo siguiente, la selección de las etiquetas de acceso a los recursos es un método sencillo para seleccionar los seis informes que contienen esta etiqueta.

Captura de pantalla del asistente de programación de informes, paso 1: Selección de informes. El título de la ventana es "Selección de informes". Debajo del título, hay un mensaje: "Seleccione los informes individualmente o por etiqueta.".

En la sección "Nombre de tarea:", hay un campo de texto vacío y un botón de verificación (checkbox) activado.

En la sección "Tipo de selección:", hay dos opciones: "Informes" (radio desactivado) y "Etiquetas" (radio activado).

Debajo de "Etiquetas", hay una lista de "Etiquetas disponibles" y una lista de "Etiquetas seleccionadas".

La lista "Etiquetas disponibles" contiene:

- HIPAA [2]
- ISO\IEC 27001\2 [7]
- JPIPA [7]
- JSOX [1]
- NERC [5]
- NISPOM [1]
- PCI [7]
- Resource Access [9] (seleccionado)
- SOX [1]

La lista "Etiquetas seleccionadas" contiene:

- Resource Access

Debajo de "Informes", hay una lista de "Informes disponibles" que incluye:

- Actividad de recurso de administración
- Actividad de acceso a los archivos de EPHI
- Actividad de control de acceso a los archivos de EPHI
- Acceso a los recursos por acción
- Acceso a los recursos por host críticos para el negocio
- Acceso a los recursos por host
- Acceso a los recursos por nombre de registro
- Acceso a los recursos por ejecutor
- Acceso a los recursos por nombre de recurso

3. (Opcional) Haga clic en Filtros de informe y cree un filtro de eventos nuevo para limitar el informe a los datos que necesita.

4. (Opcional) Haga clic en Condiciones del resultado y seleccione un intervalo de fechas o unas condiciones del resultado para esta consulta. Por ejemplo, para buscar eventos que se produjeron en las últimas seis horas, seleccione 'Ahora' como hora de finalización dinámica, y 'Ahora' y 'Últimas 6 horas' como hora de inicio dinámica. Seleccione un límite de filas y un número, como 250.

Intervalo de fechas y condiciones de resultado

Seleccione el intervalo de fechas válido y las condiciones de resultado para esta consulta.

Selección de intervalo de fechas

Seleccione un intervalo de fechas para los eventos resultantes.

Intervalos predefinidos:

Tiempo de finalización dinámico:

Tiempo de inicio dinámico:

Resultados

Seleccione los parámetros que se desea mostrar del resultado.

☐ Límite de filas: 1

☐ Mostrar otros

☐ Granularidad de tiempo: event_datetime

Condiciones de resultado

Seleccione las condiciones de resultado para los eventos agrupados.

☐ Primeros eventos agrupados con fecha posterior a:

☐ Últimos eventos agrupados con fecha posterior a:

☐ Últimos eventos agrupados con fecha anterior a:

☐ Con por lo menos 1 eventos agrupados

☐ Con no más de 1 eventos agrupados

5. Haga clic en Tareas programadas para programar la generación de Ahora o seleccione otra opción y especifique los detalles.

6. Haga clic en Destino y especifique si desea que el formato del informe sea una hoja de datos de Excel, un PDF o un XML. Una hoja de datos es adecuada para datos en forma de tabla. Un PDF es adecuado para gráficos. También puede enviar una notificación por correo electrónico. (Utilice comas como delimitadores entre las direcciones de correo electrónico.) El correo electrónico se puede enviar sin el informe para confirmar que se ha generado el informe programado, o también se puede enviar el informe como un archivo adjunto al correo electrónico.

Destino de informe

Selecione la casilla de verificación para especificar la dirección de correo electrónico.

Formato de informe: PDF

☒ Activar notificación por correo electrónico

Enviar correo a:

Desde:

Asunto:

Texto de correo electrónico:

Adjuntar informe:

☐

Nota: El administrador puede establecer que los informes se eliminen tras un período de retención determinado. El almacenamiento de una copia del correo electrónico puede emplearse como copia de seguridad alternativa con respecto al almacenamiento manual.

7. Haga clic en Selección de servidor, seleccione uno o varios servidores para los informes e indique si desea enviar una consulta a la federación del servidor.
8. Haga clic en Guardar y cerrar.

Los informes seleccionados quedan programados para su generación.

Tareas programadas				
Nombre de tarea ▲	Servidor	Repetición	Hora programada	Creador
All Resource Access Reports	caelm5	Ahora	Thu Sep 24 2009 8:10:13 am	Auditor1

Ejemplo: Enviar por correo electrónico de forma diaria informes de PCI en formato PDF

Puede automatizar el envío de determinados informes en el formato que desee a la persona que especifique y con la frecuencia necesaria.

Antes de que pueda especificar que los informes programados se guarden en formato PDF y se adjunten a mensajes de correo electrónico, debe configurar los ajustes siguientes en la configuración del servicio global del servidor de informes en la ficha Administración y en la subficha Servicios.

- Opciones del servidor de correo:
 - Servidor de correo electrónico
 - Puerto SMTP (25)
 - Correo electrónico de admin
 - Nombre de usuario y contraseña de SMTP
- Especificaciones del PDF:
 - Nombre de producto/compañía
 - URL del logotipo de producto/compañía
 - Tamaño de la fuente y de la fuente de encabezado
 - Tamaño de la fuente y de la fuente de datos
 - Orientación, ancho y alto de página

Ejemplo: Enviar todos los informes de PCI diarios, en formato PDF, al buzón de correo del auditor cada día de la semana

1. Haga clic en la ficha Informes programados y, a continuación, en la subficha Programación de informes.

Aparece la barra de herramientas con un botón de programación de informe.
2. Haga clic en Programar un informe.

Aparece el paso de selección de informes.
3. Seleccione un informe del modo que se indica a continuación:
 - a. Escriba Informes de PCI como nombre de la tarea.
 - b. Seleccione Etiquetas como tipo de selección.
 - c. Seleccione PCI en Etiquetas disponibles y desplácelo a Etiquetas seleccionadas.

4. Programe la tarea como se indica a continuación:
 - a. Haga clic en el paso de programación de tareas.
 - b. Seleccione Diario como frecuencia.
 - c. Seleccione todos los días de la semana.
5. Especifique el destino y el formato del informe del modo siguiente:
 - a. Haga clic en la ficha Destino.
 - b. Acepte el formato de informe predeterminado: PDF.
 - c. Seleccione Activar notificación por correo electrónico.
 - d. Introduzca la dirección de correo electrónico del auditor. Emplee la sintaxis siguiente: <nombre_correo>@<empresa>.com
 - e. Seleccione Adjuntar informe.
6. Haga clic en Guardar y cerrar.

Edición de tareas de informes programadas

Puede editar las tareas de informes programadas.

Para editar tareas de informes programadas

1. Haga clic en la ficha Informes programados.

Aparece la lista de servidores de informes.
2. Seleccione el servidor en el que se ha programado el informe que desea editar.

El servidor seleccionado aparece en el panel de detalles del servidor de informes.
3. Seleccione la tarea de informe que desea y haga clic en el botón Editar, situado en la parte superior de la lista.

Aparece el asistente de programación de informes.
4. Realice los cambios que desee y haga clic en Guardar y cerrar.

El informe editado aparece en la lista de tareas programadas en 5 minutos, en cuanto se actualiza la lista. Haga clic en Actualizar para mostrarlo de forma inmediata.

Más información:

[Programación de tareas de informes](#) (en la página 506)

[Eliminación de tareas de informes programadas](#) (en la página 524)

Activación y desactivación de tareas de informes programados

Puede desactivar una o varias tareas de informes programados si no desea que se ejecuten las consultas asociadas con ese informe. También se pueden activar tareas de informes programados que se desactivaron anteriormente, de manera que se puedan ejecutar de acuerdo con la programación guardada.

Para activar o desactivar tareas de informes programados

1. Haga clic en la ficha Informes programados y, a continuación, en la subficha Programación de informes.

Aparecerá la lista Tareas programadas que mostrará el estado de cada tarea en la columna Activado. Si la tarea está activada, se aplicará el valor Activado. Si está desactivada, no se aplicará el valor Activado.

2. Seleccione la tarea o las tareas que desee y haga clic en Activar seleccionados o Desactivar seleccionados.

La lista Tareas programadas mostrará el nuevo estado de todas las tareas que haya activado o desactivado.

Nota: La capacidad para desactivar tareas de informe está diseñada para uso con informes repetidos. Si desactiva una tarea de informe con una sola aparición ("Una vez"), se eliminará de la lista Tareas programadas.

Eliminación de tareas de informes programadas

Puede eliminar tareas de informes programadas.

Para eliminar tareas de informes programadas

1. Haga clic en la ficha Informes programados.

Aparece la lista de servidores de informes.

2. Seleccione el servidor en el que se ha programado el informe que desea eliminar.

El servidor seleccionado aparece en el panel de detalles del servidor de informes.

3. Haga clic en la ficha Programación de informes, seleccione la tarea deseada en la fila y haga clic en Suprimir en la parte superior de la lista. Puede seleccionar varias tareas para suprimirlas.

Nota: Las casillas de verificación que se encuentran junto a cada tarea de informes permiten activar o desactivar tareas de informes.

Aparecerá un cuadro de diálogo de confirmación.

4. Haga clic en Sí.

La tarea de informe se elimina de la lista de tareas programadas.

Más información:

[Programación de tareas de informes](#) (en la página 506)

[Edición de tareas de informes programadas](#) (en la página 522)

Eventos autocontrolados

La mayoría de las acciones del usuario generan eventos autocontrolados. Estos eventos permiten realizar un seguimiento de las acciones que se han realizado o que afectan al servidor, así como de su éxito o error. Los eventos autocontrolados se muestran en formato de visor de eventos de cada servidor en las fichas Informes programados y Gestión de alertas. También se pueden considerar como informes normales o programados mediante el informe de eventos autocontrolados.

Más información

[Visualización de eventos autocontrolados](#) (en la página 525)

[Programación de tareas de informes](#) (en la página 506)

Visualización de eventos autocontrolados

Puede visualizar eventos autocontrolados relevantes para cada servidor desde las fichas Gestión de alertas e Informes programados. Las visualizaciones de cada ficha se filtran para mostrar los eventos de control de informes o de alertas relevantes. Puede eliminar el filtro para mostrar todos los eventos autocontrolados.

Para ver eventos autocontrolados

1. Haga clic en la ficha Informes programados o en la ficha Gestión de alertas.

Aparece la lista de servidores de informes o alertas.

2. Seleccione el servidor cuyos eventos autocontrolados locales desea visualizar.

El servidor que seleccione se mostrará en el panel de detalles.

3. Haga clic en la ficha Eventos autocontrolados.

Aparece el panel del visor de eventos autocontrolados, que muestra los eventos autocontrolados relacionados con alertas o informes. Puede realizar cualquiera de las tareas normales de informes desde el panel de eventos autocontrolados, incluidas las siguientes:

- Tareas del visor de eventos
- Filtrado global o local
- Establecimiento de favoritos
- Exportación

Capítulo 14: Supresión y resumen

Esta sección contiene los siguientes temas:

[Versiones de componentes de refinamiento de eventos](#) (en la página 527)

[Tareas de reglas de resumen y supresión](#) (en la página 528)

[Creación de la regla de supresión del evento de Windows 560](#) (en la página 552)

Versiones de componentes de refinamiento de eventos

CA Enterprise Log Manager retiene versiones anteriores de determinados componentes de refinamiento de eventos personalizados a medida que los crea y los edita. Esto le permite emplear como referencia versiones anteriores. Puede visualizar o copiar versiones de los componentes siguientes:

- Archivos de análisis de mensajes
- Archivos de asignación de datos
- Reglas de supresión
- Reglas de resumen

Cada vez que crea un componente personalizado nuevo, se le asigna la versión 1.0. Al editar y guardar una versión nueva de dicho objeto, se le asigna la versión 2.0. Ambas versiones aparecen en el área de la interfaz correspondiente para su selección y aplicación.

Por ejemplo, si crea una regla de supresión personalizada denominada "NuevaRegla", aparece como NuevaRegla versión 1.0 en la lista de la interfaz del almacenamiento de registro de eventos para su aplicación. Si, posteriormente, edita dicho archivo, aparece como NuevaRegla versión 2.0 en la lista del almacenamiento de registro de eventos.

Puede visualizar versiones anteriores de componentes de refinamiento de eventos en la lista correspondiente. Dichos componentes son de sólo lectura y no se pueden editar. Puede copiar una versión antigua y editarla, convirtiéndola de este modo en una versión nueva. Por ejemplo, si nos basamos en el ejemplo anterior, no puede editar NuevaRegla versión 1.0 una vez que existe la versión 2.0. Tendría que copiar la versión 1.0 y editarla. Al guardar estas ediciones, se crea la versión 3.0.

Más información

[Edición de reglas de resumen o supresión](#) (en la página 548)

Tareas de reglas de resumen y supresión

Las reglas de resumen y supresión le permiten controlar el flujo de eventos y administrar el tamaño del almacenamiento de registro de eventos mediante la eliminación o la combinación de determinados eventos. Las reglas de supresión evitan que se registren eventos nativos que coincidan con sus calificaciones. Las reglas de resumen combinan múltiples eventos nativos en un único evento refinado que aparece en lugar de los eventos de los componentes originales.

Importante: Debe crear y emplear las reglas de resumen y supresión con precaución, ya que pueden evitar el registro y la aparición de algunos eventos nativos. Le recomendamos que compruebe las reglas de resumen y supresión personalizadas en un entorno de prueba antes de implementarlas.

Las tareas de resumen y supresión se pueden llevar a cabo desde la zona de recopilación de registros de la interfaz. Puede crear, editar y eliminar reglas de resumen y supresión personalizadas.

Más información

[Creación de reglas de supresión](#) (en la página 530)

[Creación de reglas de resumen](#) (en la página 536)

[Aplicación de reglas de resumen o supresión](#) (en la página 543)

[Copia de reglas de resumen o supresión](#) (en la página 547)

[Edición de reglas de resumen o supresión](#) (en la página 548)

[Eliminación de reglas de resumen o supresión](#) (en la página 549)

[Importación de reglas de resumen o supresión](#) (en la página 550)

[Exportación de reglas de resumen o supresión](#) (en la página 551)

Efectos de las reglas de supresión

Durante la planificación, es posible que desee tener en cuenta los efectos de las *reglas de supresión*, que evitan que los eventos se introduzcan en el sistema de almacenamiento de registro de eventos o que se recopilen mediante un conector. Las reglas de supresión siempre están vinculadas a un conector. Puede aplicar las reglas de supresión en el ámbito del agente, del grupo o del propio servidor de CA Enterprise Log Manager. Las ubicaciones tienen diferentes efectos:

- Las reglas de supresión aplicadas a los agentes o a los grupos evitan que los eventos se recopilen y, por lo tanto, reducen el volumen de tráfico de red *enviado* al servidor de CA Enterprise Log Manager.
- Las reglas de supresión aplicadas al servidor de CA Enterprise Log Manager evitan que los eventos se *inserten* en la base de datos y, por lo tanto, reducen la cantidad de información almacenada.

Existen consideraciones de rendimiento potencial a la hora de aplicar reglas de supresión a eventos una vez que hayan llegado al servidor de CA Enterprise Log Manager, especialmente si crea múltiples reglas de supresión o la tasa de flujo de eventos es elevada.

Por ejemplo, puede que desee eliminar *algunos* de los eventos de un cortafuegos o de algunos servidores de Windows que producen eventos duplicados para una misma acción. La no recopilación de estos eventos puede acelerar la transmisión de los registros de eventos que desea guardar y reduce el tiempo de procesamiento en el servidor de CA Enterprise Log Manager. En estos casos, aplicaría una o varias reglas de supresión adecuadas en los componentes del agente.

Si deseara suprimir todos los eventos de determinado tipo en múltiples plataformas o en todo el entorno, aplicaría una o varias reglas de supresión adecuadas en el servidor de CA Enterprise Log Manager. La evaluación de eventos con respecto a la supresión se produce cuando los eventos llegan al servidor de CA Enterprise Log Manager. La aplicación de un gran número de reglas de supresión en el servidor puede provocar un rendimiento más lento, ya que el servidor tiene que aplicar reglas de supresión, además de insertar eventos en el sistema de almacenamiento de registro de eventos.

Para implementaciones más pequeñas, puede llevar a cabo la supresión en el servidor de CA Enterprise Log Manager. También puede decidir aplicar la supresión en el servidor en el caso de implementaciones en las que se emplean resúmenes (acumulaciones). Si sólo introduce algunos de los eventos de un origen de eventos que genera grandes cantidades de información, puede decidir suprimir los eventos no deseados en el agente o en el grupo de agentes para reducir el tiempo de procesamiento del servidor de CA Enterprise Log Manager.

Creación de reglas de supresión

Puede emplear reglas de supresión para evitar que grandes cantidades de rutinas o transacciones conocidas y previstas aumenten el contenido del sistema de almacenamiento de registro de eventos y desorganicen la imagen de su entorno. Por ejemplo, podría emplear una regla de supresión para eliminar los eventos de información syslog no necesarios, especialmente en casos en los que no puede configurar el origen de evento para que sólo envíe el conjunto deseado.

El proceso de creación de una regla de supresión mediante el asistente para reglas de supresión consta de los pasos siguientes:

1. Apertura del asistente para reglas de supresión.
2. Nombramiento de reglas: introducción de información sobre el nombre de una regla y sobre su descripción.
3. Selección del evento: identificación de un evento para suprimirlo mediante los atributos de normalización de gramática de eventos comunes y el filtrado avanzado opcional.

Nota: Una vez que ha creado una regla de supresión, debe aplicarla para que se pueda emplear en su entorno.

Más información

[Apertura del asistente de supresión](#) (en la página 531)

[Nombramiento de una regla de supresión](#) (en la página 531)

[Aplicación de reglas de resumen o supresión](#) (en la página 543)

Apertura del asistente de supresión

Para crear una regla de supresión nueva o editar una existente, abra el asistente de supresión.

Para abrir el asistente de supresión

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Supresión y resumen.

Los botones de supresión y resumen aparecen en el panel de detalles.

3. Haga clic en Nueva regla de supresión: 

Se abre el asistente de supresión.

Al emplear el asistente:

- Haga clic en Guardar para guardar el archivo de la regla sin cerrar el asistente.
- Haga clic en Guardar y Cerrar para guardar el archivo de la regla y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Más información

[Nombramiento de una regla de supresión](#) (en la página 531)

Nombramiento de una regla de supresión

Debe asignar un nombre a cada regla de supresión. También puede introducir información descriptiva opcional como referencia.

Para nombrar una regla de supresión

1. Abra el asistente de supresión.
2. Introduzca un nombre para la regla nueva.
3. (Opcional) Introduzca información descriptiva.
4. Vaya al paso de filtrado.

Más información

[Creación de reglas de supresión](#) (en la página 530)

Selección de eventos para su supresión

Debe especificar el evento nativo al que desea aplicar la regla de supresión; para ello, configure un filtro simple para los campos de normalización de eventos de la gramática de eventos comunes. Estos cuatro campos, que forman parte de la clase específica de eventos, se ofrecen para todos los eventos de la gramática de eventos comunes y permiten identificar un evento nativo de forma precisa.

Puede especificar la combinación de campos de normalización de eventos que desee mediante la ficha Filtros simples. También puede emplear filtros avanzados para obtener información más detallada en la identificación de eventos. Debe especificar al menos un filtro simple para una regla de supresión.

Para seleccionar eventos de reglas de supresión

1. Abra el asistente de supresión, introduzca la información necesaria y vaya al paso de filtrado.
2. Cree filtros simples para seleccionar el evento que desee; para ello, seleccione la casilla de verificación correspondiente y seleccione o introduzca el valor en cuestión. Los campos disponibles son los siguientes:

Modelo ideal

Describe el tipo de tecnología relacionada con el evento, por ejemplo, cortafuegos o dispositivo de red.

Categoría de evento

Describe categorías de eventos amplias dentro del modelo ideal. Por ejemplo, todos los eventos de cuenta, de grupo de usuarios y los relacionados con funciones se registran en la categoría de evento "Gestión de identidades". Cada categoría de evento cuenta con una o más clases (subcategorías), de manera que cualquier opción seleccionada modifica las selecciones disponibles en el menú Clase de evento.

Clase de evento

Ofrece una clasificación de eventos más detallada en una categoría de evento específica. Por ejemplo, los eventos de la gestión de identidades se dividen en tres clases: cuenta, grupo o identidad. Cada clase de evento cuenta con una o más acciones asociadas, de manera que cualquier opción seleccionada modifica las selecciones disponibles en el menú Acción de evento.

Acción de evento

Describe acciones habituales de cada clase y categoría de evento. Por ejemplo, la gestión de cuentas, que es una clase de la categoría de gestión de identidades, cuenta con acciones de creación, eliminación y modificación de cuentas.

3. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la regla nueva aparece en la lista; si no es así, aparece el paso que haya seleccionado.

Cuando crea una regla nueva, se guarda como versión 1.0. Si, posteriormente, la edita, se almacena una copia independiente de la regla como una versión nueva. Puede visualizar versiones anteriores, así como aplicarlas y copiarlas según desee.

Más información:

[Creación de un filtro de evento simple](#) (en la página 594)

[Creación de filtros de eventos avanzados](#) (en la página 597)

[Uso de filtros avanzados](#) (en la página 533)

Uso de filtros avanzados

Puede emplear filtros avanzados para calificar cualquier consulta relacionada con supresiones o resúmenes del almacén de registro de eventos. La interfaz Filtros avanzados le ayuda a crear la sintaxis apropiada para los filtros proporcionando un formulario para introducir columnas, operadores y valores lógicos en función de los requisitos de las reglas de supresión o resumen.

Nota: Esta sección contiene una breve descripción general de los términos empleados en los filtros avanzados para reglas de supresión y de resumen. Para aprovechar al máximo el potencial de los filtros avanzados, debe conocer a fondo los términos del filtro y la gramática de eventos comunes.

Los siguientes términos unen varias instrucciones de filtros:

And

Muestra la información del evento si *todos* los términos unidos son verdaderos.

Or

Muestra la información del evento si *cualquiera* de los términos unidos es verdadero.

Los filtros avanzados utilizan los siguientes operadores SQL para crear las condiciones básicas para las supresiones o los resúmenes:

Match

Incluye cualquier información del evento que coincida con uno o más de los caracteres de la cadena alfanumérica introducida, de manera que se puede buscar por palabra clave. Este tipo de búsqueda distingue entre mayúsculas y minúsculas.

Match (ignore case)

Incluye cualquier información del evento que coincida con uno o más de los caracteres de la cadena alfanumérica introducida, de manera que se puede buscar por palabra clave. Este tipo de búsqueda no distingue entre mayúsculas y minúsculas.

Not Match

Incluye cualquier información del evento que no coincida con uno o varios de los caracteres de la cadena alfanumérica introducida. Este tipo de búsqueda distingue entre mayúsculas y minúsculas.

Not Match (ignore case)

Incluye cualquier información del evento que no coincida con uno o varios de los caracteres de la cadena alfanumérica introducida. Este tipo de búsqueda no distingue entre mayúsculas y minúsculas.

Regular Expression Match

Incluye cualquier información del evento que coincida con uno o varios de los caracteres de expresión regular introducidos. Puede utilizarse para realizar búsquedas en un entorno multibyte y con comodines.

Not Regular Expression Match

Incluye cualquier información del evento que no coincida con uno o varios de los caracteres de expresión regular introducidos. Puede utilizarse para realizar búsquedas en un entorno multibyte y con comodines.

Operadores relacionales

Incluye la información del evento si la columna tiene la relación apropiada con el valor introducido. Dispone de los siguientes operadores relacionales:

- Equal to (numérico)
- Not Equal to (numérico)
- Greater than (numérico)
- Greater than or equal to (numérico)
- Less than (numérico)

- Less than or equal to (numérico)

Por ejemplo, si usa *Greater than*, incluiría la información del evento de la columna seleccionada si su valor fuera mayor que el valor especificado.

Todos estos operadores sólo encuentran números; para buscar otros caracteres, seleccione uno de los operadores "match", según proceda.

Creación de reglas de resumen

Puede emplear las reglas de resumen para combinar determinados eventos nativos de tipo común en un evento refinado. Esto le permite ahorrar espacio en el sistema de almacenamiento de registro de eventos y simplifica el análisis de eventos.

Por ejemplo, puede crear una regla de resumen que registre un único evento refinado cada tres intentos fallidos de inicio de sesión por parte de un usuario. Esto significa que el sistema de almacenamiento de registro de eventos registra un solo evento en lugar de tres.

El proceso de creación o edición de reglas de resumen mediante el asistente para reglas de resumen consta de los siguientes pasos principales:

1. Apertura del asistente para reglas de resumen.
2. Umbrales de resumen: configuración del número o frecuencia de eventos nativos con los que desea crear un evento resumido.
3. Selección del evento: identificación de un evento para resumirlo mediante los atributos de normalización de gramática de eventos comunes y el filtrado avanzado opcional.
4. Resumen: control de la presentación del evento resumido final en los informes.

Nota: Una vez que ha creado una regla de resumen, debe aplicarla para que se pueda emplear en su entorno.

Más información

[Apertura del asistente de resumen](#) (en la página 537)

[Establecimiento de umbrales de resumen](#) (en la página 537)

[Configuración de visualizaciones de resúmenes](#) (en la página 541)

[Aplicación de reglas de resumen o supresión](#) (en la página 543)

Apertura del asistente de resumen

Para crear una regla de resumen nueva o editar una existente, abra el asistente de resumen.

Para abrir el asistente de supresión

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Supresión y resumen.

Los botones de supresión y resumen aparecen en el panel de detalles.

3. Haga clic en Nueva regla de resumen: 

Se abre el asistente de resumen.

Al emplear el asistente:

- Haga clic en Guardar para guardar el archivo de la regla sin cerrar el asistente.
- Haga clic en Guardar y Cerrar para guardar el archivo de la regla y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Más información

[Establecimiento de umbrales de resumen](#) (en la página 537)

[Configuración de visualizaciones de resúmenes](#) (en la página 541)

Establecimiento de umbrales de resumen

Para crear o editar una regla de resumen, introduzca información general y establezca umbrales de resumen. Los umbrales son un determinado número de eventos, una frecuencia de repetición o una combinación de ambos que activa la creación de un evento de resumen.

Para establecer umbrales de resumen

1. Abra el asistente de resumen.
2. Introduzca un nombre para la regla nueva. También puede introducir información descriptiva opcional como referencia.

3. Defina la combinación mediante la especificación del número de eventos nativos y el tiempo transcurrido que emplea la regla para crear un evento refinado único a través de las opciones de resumen del evento:

Activación del umbral de recuento de eventos

Controla si la regla emplea o no un umbral de eventos. El umbral de eventos debe ser superior a uno. La selección de esta casilla establece un valor máximo de eventos. Si no se selecciona esta casilla y se activa el período de tiempo de espera de eventos, sólo se tendrá en cuenta el período de tiempo de resumen de eventos. Si se activan ambos, se crea un evento resumido tras cada período de tiempo especificado, siempre y cuando se produzca al menos un evento sin formato calificado.

Número máximo de eventos

Define el número de eventos nativos que activan un evento resumido. Cuando se alcanza el número de eventos nativos especificado, se crea un evento resumido.

Mínimo: 2

Máximo: 5.000

Activación del período de tiempo de espera de eventos

Controla si la regla emplea o no un umbral de período de tiempo. La selección de esta casilla establece un valor de período de tiempo. Si no se selecciona esta casilla, el evento resumido sólo se produce cuando se alcanza el umbral de recuento de eventos.

Período de tiempo

Define el tiempo, en segundos, que transcurre para activar un evento resumido, en caso de que se produzca alguno de los eventos del tipo especificado. Al alcanzar este umbral, se crea un evento resumido, siempre y cuando se haya producido al menos un evento nativo calificado. Puede definir el período de tiempo como cero, que sólo da como resultado un evento resumido cuando se alcanza el umbral máximo de eventos.

Mínimo: 0

Máximo: 86.400

Por ejemplo, en el caso de una regla que resume los intentos de inicio de sesión erróneos, la selección de 3 en el menú Número máx. de eventos y de 10 en el menú Período de tiempo da como resultado un evento resumido después de tres intentos de inicio de sesión erróneos o cada 10 segundos, siempre y cuando se produzca al menos un inicio de sesión erróneo.

4. Haga clic en la flecha correspondiente para avanzar al paso del asistente que quiera completar a continuación o haga clic en Guardar y cerrar.
Si hace clic en Guardar y cerrar, la regla nueva aparece en la lista; si no es así, aparece el paso que haya seleccionado.

Más información

[Configuración de visualizaciones de resúmenes](#) (en la página 541)

Selección de eventos para su resumen

Especifique el evento nativo al que desea aplicar la regla de resumen mediante la configuración de un filtro simple para los campos de normalización de eventos de la gramática de eventos comunes. Estos cuatro campos, que forman parte de la clase específica de eventos, se ofrecen para todos los eventos de la gramática de eventos comunes y facilitan la identificación de eventos.

Puede especificar la combinación de campos de normalización de eventos deseada mediante la ficha Filtros simples. También puede emplear filtros avanzados para obtener información más detallada en la identificación de eventos. Especifique al menos un filtro simple para una regla de supresión.

Para seleccionar eventos de reglas de resumen

1. Abra el asistente de resumen y vaya al paso de filtrado.
2. Cree filtros simples para seleccionar el evento deseado. Para ello, seleccione la casilla de verificación correspondiente y, a continuación, seleccione o introduzca el valor que desee. Los campos disponibles son los siguientes:

Modelo ideal

Describe de forma general la clase de tecnología implicada en el evento. Por ejemplo, Cortafuegos y Dispositivo de red son modelos ideales.

Categoría de evento

Describe de forma general las categorías de los eventos. Por ejemplo, todos los eventos de cuenta, de grupo de usuarios y los relacionados con funciones se registran en la categoría de evento "Gestión de identidades". Cada categoría de evento cuenta con una o más clases (subcategorías), de manera que cualquier opción modifica las selecciones disponibles en el menú Clase de evento.

Clase de evento

Ofrece una clasificación de eventos más detallada en una categoría de evento específica. Por ejemplo, los eventos de la gestión de identidades se dividen en tres clases: cuenta, grupo o identidad. Cada clase de evento cuenta con una o más acciones asociadas, de manera que cualquier opción modifica las selecciones disponibles en el menú Acción de evento.

Acción de evento

Describe acciones habituales de cada clase y categoría de evento. Por ejemplo, la gestión de cuentas, que es una clase de la categoría de gestión de identidades, cuenta con acciones de creación, eliminación y modificación de cuentas.

3. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la regla nueva aparece en la lista; si no es así, aparece el paso que haya seleccionado.

Más información:

[Creación de un filtro de evento simple](#) (en la página 594)

[Creación de filtros de eventos avanzados](#) (en la página 597)

[Configuración de visualizaciones de resúmenes](#) (en la página 541)

[Establecimiento de umbrales de resumen](#) (en la página 537)

Configuración de visualizaciones de resúmenes

Las reglas de resumen controlan cómo se muestran los eventos nativos en el evento refinado. La configuración de las visualizaciones de resúmenes se realiza seleccionando Resumen por campos y Campos agregados.

Para configurar visualizaciones de reglas de resumen

1. Abra el asistente de resumen y vaya al paso de resumen.
2. Seleccione los campos mediante los que desee resumir el evento refinado a través del control de cambio:

Resumen por

Controla los campos por los que se agrupa la información resumida. Por ejemplo, en el caso de una regla que resume los registros erróneos, seleccione `source_username` para mostrar el número de eventos de inicio de sesión errónea calificados para cada usuario por separado. Debe seleccionar uno o más campos Resumen por para completar la regla.

3. (Opcional) Seleccione los campos por los que desea agregar el evento refinado:

Agregado

Controla los campos por los que se subdivide la información resumida, en función del campo Resumido por. Por ejemplo, en el caso de una regla que resume los inicios de sesión erróneos, seleccione `source_username` como campo de Resumido por, y `dest_hostname` como campo de Agregado. Esto muestra el número de eventos de inicio de sesión erróneo calificados de cada usuario por separado, subdivididos según el host en el que trató de iniciar sesión el usuario.

La información de los campos agregados se retiene en el campo de eventos sin formato de los eventos resumidos. En el ejemplo anterior, cada host en el que el usuario trató de iniciar sesión se almacenará con el número de repeticiones con el formato siguiente:

nombrehost1:2,nombrehost2:5. Este ejemplo muestra 2 intentos de inicio de sesión del host 1 y 5 intentos del host 2.

Los campos de Agregado son opcionales; no tiene que seleccionar un campo en Agregado para finalizar la regla.

4. Haga clic en la flecha correspondiente para avanzar al paso del asistente que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la regla nueva aparece en la lista; si no es así, aparece el paso que haya seleccionado.

Cuando crea una regla nueva, se guarda como versión 1.0. Si, posteriormente, la edita, se almacena una copia independiente de la regla como una versión nueva. Puede visualizar versiones anteriores, así como aplicarlas y copiarlas según desee.

Más información

[Establecimiento de umbrales de resumen](#) (en la página 537)

Aplicación de reglas de resumen o supresión

Una vez que ha creado una regla de resumen o supresión, debe aplicarla para que se pueda emplear en su entorno. Esta función ayuda a evitar la aplicación de reglas de resumen o supresión sin llevar a cabo la comprobación y la aprobación adecuadas.

Para aplicar reglas de resumen o supresión

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.

Aparece la lista de servicios.

2. Haga clic en el icono de almacenamiento de registro de eventos.

Aparece el panel de configuración Almacenamiento de registro de eventos.

3. Busque y seleccione la regla de resumen o supresión que desee aplicar mediante el control de cambio adecuado.

4. Haga clic en Guardar.

Si la regla se aplica de forma correcta, aparece un mensaje de confirmación.

Aplicación de supresiones y resúmenes en componentes de agentes

Puede asignar reglas de supresión, de resumen o ambas a grupos de agentes, agentes o conectores del entorno. Estas reglas pueden sustituir o complementar cualquier regla de supresión o resumen aplicada en el servidor de CA Enterprise Log Manager. Por lo tanto, puede agilizar el proceso de transmisión/recepción de eventos a través del control del lugar en el que se produce el refinamiento.

Por ejemplo, si tiene un grupo de agentes de Windows, puede asociar una regla de supresión que elimine los eventos de Windows innecesarios para los agentes del grupo. De este modo, evita la necesidad de que todos los eventos entrantes se sometan a una comprobación específica de Windows en el servidor de CA Enterprise Log Manager.

Puede aplicar reglas de supresión o resumen en diferentes niveles de la jerarquía de carpetas de agentes:

- En la carpeta Explorador de agente, puede aplicar reglas a grupos de agentes, agentes individuales o conectores.
- Desde la carpeta de un grupo de agentes determinado, puede aplicar reglas a todos los agentes de dicho grupo y a todos los conectores asignados a ellos.
- Desde un agente individual, sólo puede aplicar reglas a dicho agente y a los conectores asignados a él.

El proceso de aplicación de reglas de supresión o resumen en los componentes del agente consta de los pasos siguientes:

1. Apertura del asistente de gestión de reglas.
2. Selección de destinos; grupos de agentes, agentes o conectores.
3. Selección de las reglas de supresión que se van a aplicar.
4. Selección de las reglas de resumen que se van a aplicar.

También puede eliminar reglas de supresión o resumen de múltiples grupos de agentes, agentes o conectores que emplean el asistente de gestión de reglas.

Más información:

[Apertura del asistente de gestión de reglas de resumen](#) (en la página 544)

[Selección de destinos de supresión y resumen](#) (en la página 545)

[Selección de reglas de supresión para su aplicación](#) (en la página 545)

[Selección de las reglas de resumen que se van a aplicar](#) (en la página 546)

Apertura del asistente de gestión de reglas de resumen

Para aplicar reglas de supresión o resumen a grupos de agentes, agentes individuales o recopiladores, puede usar el asistente de gestión de reglas.

Para abrir el asistente de gestión de reglas

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la carpeta Explorador de agente y, a continuación, haga clic en Gestionar reglas de resumen y supresión: 

Aparece el asistente de gestión de reglas.

Al emplear el asistente:

- Haga clic en Guardar para guardar el archivo sin cerrar el asistente.
- Haga clic en Guardar y cerrar para guardar el archivo y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Selección de destinos de supresión y resumen

Para aplicar reglas de supresión y resumen en componentes de agentes, seleccione los destinos de las reglas.

Para seleccionar los destinos

1. Abra el asistente de gestión de reglas.
2. Seleccione si desea aplicar las reglas en grupos de agentes, agentes o conectores.
3. (Opcional) Seleccione Suprimir si desea eliminar reglas en lugar de añadirlas.
4. Seleccione los destinos deseados mediante el control de cambio.

Nota: Puede buscar nombres de agentes o conectores. Si no aparecen agentes o conectores en la lista disponible, haga clic en Buscar para mostrar todos los agentes o conectores disponibles.

5. Vaya al paso de aplicación de reglas deseado.

Selección de reglas de supresión para su aplicación

Para finalizar la asignación de reglas de supresión a un grupo de agentes, un agente o un conector, seleccione qué reglas se van a aplicar.

Para seleccionar reglas de supresión

1. Abra el asistente de reglas de supresión y vaya al paso de aplicación de reglas de supresión.
2. Seleccione cuáles de las reglas disponibles desea aplicar mediante el control de cambio.

Nota: Puede buscar reglas de supresión mediante el campo Patrón de reglas de supresión.

3. Haga clic en Guardar y cerrar.

Las reglas seleccionadas se aplican a los destinos elegidos.

Selección de las reglas de resumen que se van a aplicar

Para finalizar la asignación de reglas de resumen a un grupo de agentes, un agente o un conector, seleccione qué reglas se van a aplicar.

Para seleccionar reglas de resumen

1. Abra el asistente de gestión de reglas de resumen y vaya al paso de aplicación de reglas de resumen.
2. Seleccione cuáles de las reglas disponibles desea aplicar mediante el control de cambio.

Nota: Puede buscar reglas de resumen mediante el campo Patrón de las reglas de resumen.

3. Haga clic en Guardar y cerrar si ya ha terminado de aplicar reglas.
4. Las reglas seleccionadas se aplican a los destinos elegidos. Si selecciona Suprimir en el paso de selección de destinos, las reglas seleccionadas se eliminarán.

Copia de reglas de resumen o supresión

Puede copiar reglas de resumen o supresión, lo que le permite crear una regla nueva basada en otra existente.

Para copiar reglas de resumen o supresión

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Supresión y resumen.

Los botones de supresión y resumen aparecen en el panel de detalles.

3. Haga clic en la carpeta Supresión y resumen que contiene la regla que desea copiar.

La carpeta se abre y muestra las reglas.

4. Seleccione la regla que desea copiar y haga clic en Copiar elemento seleccionado: 

Se abre el asistente de resumen o supresión y muestra la regla.

5. Realice los cambios deseados y haga clic en Guardar y cerrar.

La regla aparece en la lista correspondiente.

Edición de reglas de resumen o supresión

Puede editar reglas de resumen o supresión.

Para editar reglas de resumen o supresión

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Supresión y resumen.

Los botones de supresión y resumen aparecen en el panel de detalles.

3. Haga clic en la carpeta Supresión y resumen que contiene la regla que desea editar.

4. Seleccione la regla que desea editar y haga clic en el icono de edición de reglas de resumen o supresión.

Aparece el asistente de supresión o el asistente de resumen y muestra la regla seleccionada.

5. Realice los cambios deseados y haga clic en Guardar y cerrar.

La regla aparece en la lista correspondiente como versión nueva de la regla editada.

Más información

[Versiones de componentes de refinamiento de eventos](#) (en la página 527)

Eliminación de reglas de resumen o supresión

Puede eliminar las reglas de resumen o supresión que no sean necesarias.

Para eliminar reglas de resumen o supresión

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Supresión y resumen.

Los botones de supresión y resumen aparecen en el panel de detalles.

3. Haga clic en la carpeta Supresión y resumen que contiene la regla que desea eliminar.

4. Seleccione la regla que desea eliminar y haga clic en el icono de eliminación de reglas de resumen o supresión. Se selecciona de forma predeterminada la versión actual. Puede seleccionar una versión anterior para su eliminación en la lista desplegable Versión del panel de detalles.

Aparece un cuadro de diálogo de confirmación. Si ha aplicado la regla a una integración, aparece una advertencia. La eliminación de la regla también la elimina de la integración.

5. Haga clic en Sí.

La regla eliminada se quita de la lista correspondiente.

Importación de reglas de resumen o supresión

Puede importar reglas de supresión o resumen, ya que puede mover las reglas de un entorno a otro. Por ejemplo, podría importar reglas creadas en un entorno de prueba a un entorno real.

Para importar reglas de resumen o supresión

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la lista de la carpeta Recopilación de registros.
2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta de reglas de supresión y resumen.
En el panel de detalles, aparecen los botones Importar regla de resumen o de supresión y Exportar regla de resumen o de supresión.
3. Haga clic en Importar regla de resumen o de supresión.
Aparece el cuadro de diálogo de importación de archivo.
4. Busque el archivo que desea importar y haga clic en Aceptar.
Aparece el asistente de supresión o de resumen, que indica los detalles de la regla seleccionada.
5. Realice los cambios deseados y haga clic en Guardar y cerrar. Si la regla importada tiene el mismo nombre que otra regla que ya se encuentra en la base de datos de gestión, deberá cambiarle el nombre.
La regla importada aparece en la carpeta de supresión o de resumen correspondiente.

Exportación de reglas de resumen o supresión

Puede exportar reglas de resumen o supresión. Esto le permite compartir reglas en distintos entornos. Por ejemplo, podría exportar reglas creadas en un entorno de prueba a un entorno real.

Para exportar reglas de resumen o supresión

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la lista de la carpeta Recopilación de registros.
2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta de reglas de supresión y resumen.
Aparece el botón Exportar regla de resumen o de supresión en el panel de detalles.
3. Haga clic en la carpeta Reglas de supresión o Reglas de resumen que contiene el archivo que desea exportar.
La carpeta se expande y muestra los archivos.
4. Seleccione la regla que desea exportar y, a continuación, haga clic en Exportar regla de resumen o de supresión. Se selecciona de forma predeterminada la versión actual. Puede seleccionar una versión anterior para su exportación en la lista desplegable Versión del panel de detalles.
Aparece un cuadro de diálogo de ubicación de exportación.
5. Introduzca o busque la ubicación en la que desea almacenar la regla exportada y haga clic en Guardar.
Aparece un cuadro de diálogo de confirmación de exportación correcta.
6. Haga clic en Aceptar.
La regla se exporta.

Creación de la regla de supresión del evento de Windows 560

La activación de la auditoría de acceso de objetos en un servidor Windows crea un importante volumen de tráfico de eventos, algunos de los que quizá desee eliminar. Por ejemplo, Windows genera dos eventos cada vez que un administrador abre Microsoft Management Console (mmc.exe). Los ID de estos eventos son 560 y 562.

En este ejemplo, crea una regla nueva que suprime los eventos de Windows mediante un event_id 560. Si sigue los pasos indicados en el procedimiento siguiente, obtendrá una regla de supresión real que podrá emplear en el entorno de red, así como para demostrar cómo emplear el asistente.

Para comenzar con este ejemplo, debe iniciar sesión en un servidor de CA Enterprise Log Manager como un usuario con competencias y privilegios de administrador. No puede crear ni editar reglas de supresión si ha iniciado sesión como usuario EiamAdmin.

Para crear una regla de supresión para eventos de Windows 560

1. Abra el asistente para reglas de supresión.
2. Escriba "Supresión del evento de Windows 560" en el campo de introducción del nombre y añada la descripción siguiente: "Esta regla suprime el evento de Windows 560, ya que el SO también crea el evento 562 para el mismo tipo de acceso a los recursos. Esta retención no es necesaria para demostrar la conformidad."
3. Vaya al paso de filtrado y seleccione los siguientes filtros simples:
 - a. Valor de Modelo ideal, sistema operativo.
 - b. Valor de Categoría de evento, acceso a los recursos.
 - c. Valor de Clase de evento, recurso abierto.
 - d. Valor de Acción de evento, actividad de los recursos.

4. Haga clic en la ficha Filtros avanzados y en el botón Nuevo filtro de evento.

Aparece una nueva línea de filtro en la tabla. Puede hacer clic en un valor o en el espacio vacío de las celdas de la tabla para seleccionar un valor o introducir uno nuevo.

El campo del operador lógico tiene el valor predeterminado AND. Si dispone de varios tipos distintos de eventos que deseaba suprimir, puede introducir los ID de dichos eventos con nuevas líneas que empleen el operador lógico OR.

5. Establezca los valores de filtros de campo avanzados:

- a. Haga clic en el valor del campo Columna y seleccione el campo event_id.
- b. Haga clic en el campo Operador y seleccione Equal to.
- c. Haga clic en el campo Valor e introduzca el valor 560.

6. Haga clic en Guardar y cerrar.

El asistente crea de forma automática una carpeta Usuario que contiene las reglas de supresión. Puede ver esta carpeta al expandir la carpeta Reglas de supresión.

Capítulo 15: Asignación y análisis

Esta sección contiene los siguientes temas:

[Estados de eventos](#) (en la página 556)

[Tareas de reglas de asignación y análisis](#) (en la página 558)

[Creación de archivos de análisis de mensajes](#) (en la página 558)

[Creación de archivos de asignación de datos](#) (en la página 577)

[Tareas de reglas de transferencia de eventos](#) (en la página 592)

Estados de eventos

La información sobre los eventos de su entorno pasa por un cierto número de etapas, desde la aparición inicial hasta la posible visualización final en CA Enterprise Log Manager. Dado que el término "evento" puede hacer referencia a cualquiera de estas etapas, emplearemos la terminología siguiente para los posibles estados de eventos de su entorno:

Evento nativo

Hace referencia a la aparición inicial del estado o acción que desencadena el evento, por ejemplo, una autenticación errónea o una infracción en el cortafuegos. El servicio de escucha o conector apropiado envía los eventos nativos, los analiza y asigna según sea necesario y, a continuación, los introduce en el almacén de registro de eventos donde pueden visualizarse como eventos refinados o sin formato.

Evento sin formato

Hace referencia a la comunicación enviada por el agente de control correspondiente. Los eventos sin formato contienen información sobre el evento nativo, a menudo en forma de cadena de syslog o de par nombre-valor. Esta información se almacena y permite la realización de búsquedas, a no ser que se modifique mediante reglas de resumen o supresión. Los eventos suprimidos no se registran en el almacenamiento del registros de eventos; un conjunto de eventos resumidos se registra como un único evento que expresa el resultado del resumen.

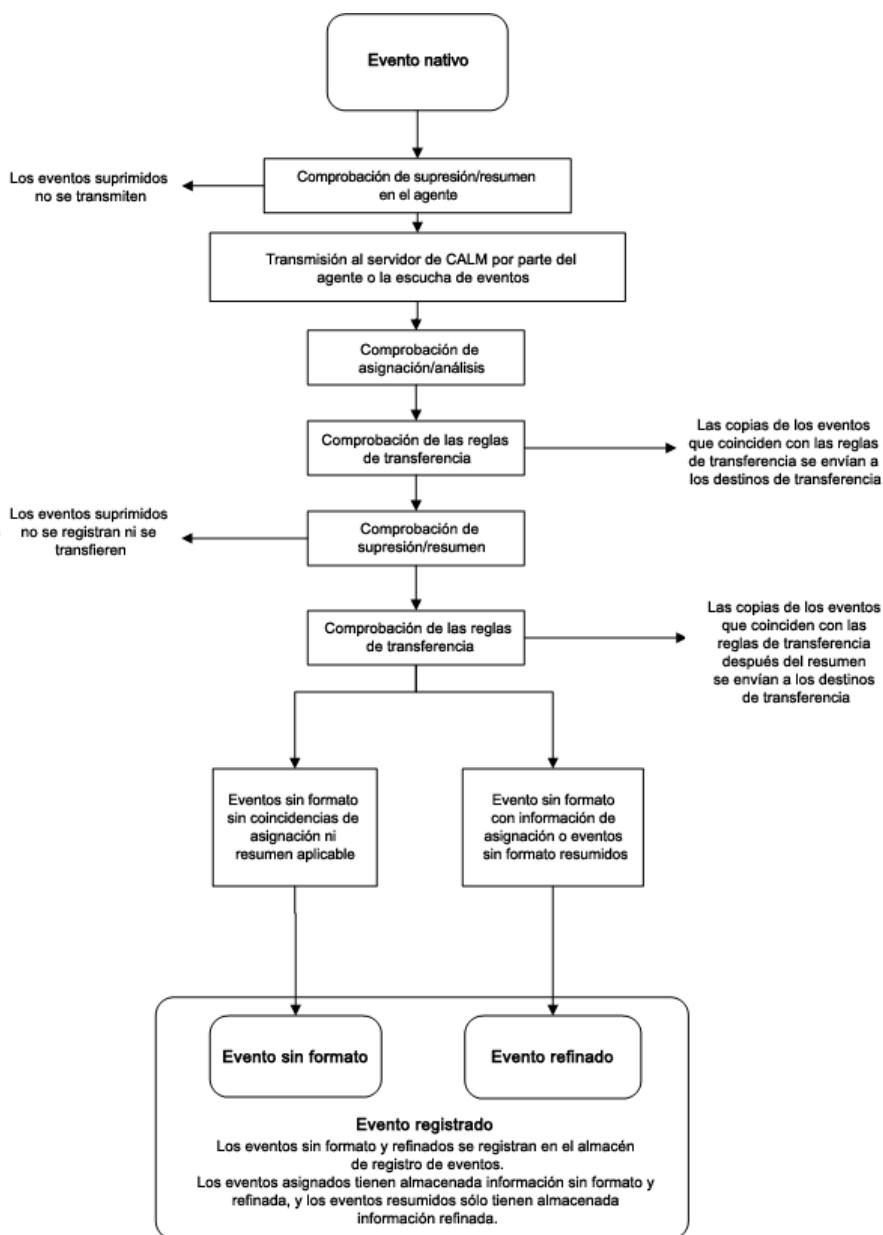
Evento refinado

Hace referencia a la información del evento asignada y resumida por CA Enterprise Log Manager. Esta información se almacena y se pueden realizar búsquedas en ella.

Evento registrado

Hace referencia a la información sobre un evento sin formato o refinado en el sistema de almacenamiento del registro de eventos. Los eventos sin formato y los eventos refinados siempre se registran, a no ser que se supriman o resuman. Los eventos asignados cuentan con información sin formato y refinada. Esta información se almacena y se pueden realizar búsquedas en ella.

Consulte el diagrama siguiente para obtener información sobre el estado de los eventos:



Más información:

[Tareas de reglas de resumen y supresión](#) (en la página 528)

[Tareas de reglas de asignación y análisis](#) (en la página 558)

Tareas de reglas de asignación y análisis

Los pares de archivos de análisis de mensajes (XMP) y asignación de datos (DM) recopilan y normalizan datos de determinados tipos de orígenes de eventos. La mayor parte de los eventos nativos entrantes pasan el análisis y, a continuación, los procesos de asignación para crear un evento del que se pueda hacer un informe y que se inserte en el almacén de registro de eventos. Los eventos transmitidos a través de SAPI o iTechnology no requieren un análisis y pasan directamente a la fase de asignación de datos.

Nota: Para aprovechar al máximo estas funciones avanzadas, debe poseer unos amplios conocimientos de los eventos sin formato y recopilados de su entorno, de los campos de destino que desea analizar, de la sintaxis de expresiones regulares, de la gramática de eventos comunes, así como de los archivos de asignación de datos y XMP, y de cómo dichos archivos analizan los eventos.

Los archivos XMP basados en XML leen datos de evento sin formato y crean pares de nombres y valores según las especificaciones que haya realizado. A continuación, los archivos de asignación de datos asignan los pares de nombres y valores de eventos creados por el análisis de mensajes a la gramática de eventos comunes. Al crear archivos de análisis y asignación nuevos, considérellos como parte de un proceso. Por ejemplo, un análisis correcto y completo permite una asignación rápida y eficaz.

Más información

[Versiones de componentes de refinamiento de eventos](#) (en la página 527)

[Creación de archivos de análisis de mensajes](#) (en la página 558)

[Creación de archivos de asignación de datos](#) (en la página 577)

Creación de archivos de análisis de mensajes

Puede emplear el asistente de archivo de análisis para crear, editar o analizar un archivo de análisis de mensajes (XMP). Los archivos de análisis leen los datos de eventos sin formato entrantes y crean pares nombre-valor, lo que le permite establecer asignaciones incluso antes de que se lleve a cabo el proceso de asignación de datos. Esto permite mejorar la eficacia general de la asignación.

Nota: Los nombres de la gramática de eventos comunes no se ven obligados a realizar el análisis de eventos, permitiendo así una mayor flexibilidad para crear pares nombre/valor. Los campos de la gramática de eventos comunes están disponibles para su selección, pero los nombres y los valores de los campos no se limitan a los valores de la gramática de eventos comunes.

La creación o edición de archivos XMP consta de los pasos siguientes:

1. Apertura del asistente de archivo de análisis
2. Ofrecimiento de detalles del archivo, incluido el nombre del archivo, el nombre del registro y la información de soporte.
3. Ubicación de eventos de muestra para la creación y comprobación de archivos.
4. Establecimiento de valores globales que se aplicarán a todos los eventos analizados por el archivo.
5. Creación o edición de cadenas de coincidencia previa para comenzar el análisis de evento.
6. Selección de filtros de coincidencia previa para adjuntar filtros de análisis.
7. Creación o edición de filtros de análisis para completar el análisis de evento.
8. Análisis y almacenamiento del archivo XMP nuevo o editado.

Más información

[Definición de detalles de archivo](#) (en la página 560)

[Carga de eventos de ejemplo](#) (en la página 562)

[Adición de campos globales](#) (en la página 563)

[Creación de filtros de coincidencia previa](#) (en la página 564)

[Análisis del archivo XMP](#) (en la página 576)

Apertura del asistente para el archivo de análisis

Para crear una regla de análisis de mensajes o editar una existente, debe abrir el asistente para el archivo de análisis.

Para abrir el asistente para el archivo de análisis

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.
2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Asignación y análisis.

Los botones de integración de productos aparecen en el panel de detalles.

3. Haga clic en Nueva regla de análisis de mensajes: 

Se abre el asistente para el archivo de análisis.

Al emplear el asistente:

- Haga clic en Guardar para guardar sin cerrar el asistente.
- Haga clic en Guardar y cerrar para guardar el archivo y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Definición de detalles de archivo

Puede agregar nuevos detalles del archivo de análisis, incluida la información de nombre, origen y referencia. Los archivos recién creados o editados se muestran en la carpeta usuario del área de asignación y análisis.

Para agregar nuevos detalles a archivos de análisis

1. Abra el asistente de archivo de análisis.
2. Especifique el área de información del archivo de análisis tal y como se indica en los subpasos siguientes:
 - a. Escriba un nombre para el archivo. El nombre de archivo es obligatorio y no puede contener los caracteres siguientes: / \ : * ? " < > ^ ; ' , & { } [] o | .
 - b. Escriba el nombre de registro de origen para identificar el nombre de registro del tipo de evento que desea que analice el archivo. La función de relleno automático muestra los nombres de registro disponibles a medida que escribe. El nombre de registro seleccionado se mostrará en el campo event_logname del evento refinado.
 - c. Agregue una descripción de referencia si lo desea.
3. (Opcional) Agregue información de soporte como referencia, tal y como se indica en los subpasos siguientes.
 - a. Haga clic en Agregar producto en el área de información de soporte. Aparece una nueva fila de información de soporte.
 - b. Haga clic en el texto Producto nuevo o Versión nueva para habilitar los campos de entrada y escriba la información de producto/versión que desee.
4. Haga clic en la flecha correspondiente para avanzar al paso del asistente que quiera completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario de archivo de análisis; si no lo hace, aparece el paso seleccionado.

Carga de eventos de ejemplo

Puede ofrecer eventos de ejemplo para emplearlos al probar archivos XMP nuevos mediante la búsqueda del almacenamiento de registro de eventos o el acceso a un archivo de registro. Los eventos de ejemplo ofrecen una plantilla con la que puede probar el archivo de análisis a medida que lo crea con los otros pasos del asistente. También puede emplear eventos de ejemplo para probar el resultado del análisis en el último paso del asistente.

Para ofrecer eventos de ejemplo

1. Abra el asistente del archivo de análisis y vaya al paso de carga de eventos. Aparece la pantalla de carga de eventos.
2. Seleccione el botón de opción Almacén de registros o Archivo de registro en el área de búsqueda de eventos de ejemplo.

- Si selecciona Almacén de registros:
 - a. Seleccione el tipo de origen de evento de ejemplo que desee en el menú desplegable Columna de análisis. Seleccione `result_string` para los orígenes de eventos WMI, o `raw_event` para los orígenes de eventos syslog.
 - b. Seleccione la consulta que desea emplear para ofrecer eventos de ejemplo mediante el filtro de etiquetas de consulta y la lista de consultas.

Aparece la consulta, que muestra eventos de ejemplo que puede emplear para probar el análisis a medida que avanza por los pasos del asistente.

Nota: Puede emplear cualquier consulta disponible o personalizada para localizar eventos de ejemplo. Si pretende utilizar una consulta personalizada, le recomendamos que la cree y la pruebe antes de comenzar el proceso de diseño del archivo de análisis de mensajes. Le recomendamos emplear un archivo de evento de ejemplo con menos de 1.500 eventos para que el análisis resulte sencillo.

- Si selecciona Archivo de registro, busque el archivo de registro deseado y haga clic en Cargar.

Los eventos del archivo de registro aparecen en el panel Eventos de ejemplo. Puede emplear los eventos para probar el análisis a medida que avanza por los pasos del asistente.

Nota: El asistente asume que cada línea del archivo es un evento. No se admiten eventos de varias líneas.

3. Haga clic en la flecha correspondiente para avanzar al paso del asistente que quiera completar a continuación.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario de archivo de análisis; si no lo hace, aparece el paso seleccionado.

Adición de campos globales

Puede agregar campos globales, que son pares estáticos que hacen coincidir un nombre de campo con un valor específico. El proceso de análisis agrega los campos globales a todos los eventos analizados, lo que mejora el uso de los valores predeterminados como modelo ideal.

Para agregar campos globales

1. Abre el asistente de archivos de análisis y se dirige al paso Campos globales. Aparecerá la pantalla Campos globales.
2. Haga clic en Agregar campo global en el área Campos globales. Aparece una fila de nuevo campo global en la tabla de campos que muestra las entradas Nuevo campo global y Nuevo valor.
3. Haga clic en el texto Nuevo campo global para introducir la información del nombre que desee. La función de autocompletado presenta nombres de campo de la Gramática de eventos comunes mientras escribe. Puede hacer clic una vez para seleccionar o escribir un nombre de campo que no sea de la Gramática de eventos comunes.
4. Haga clic en el texto Nuevo valor para introducir la información del nombre que desee.
5. Repita (opcionalmente) los pasos del 2 al 4 para agregar campos globales adicionales según sea necesario.
6. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar. Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario del archivo de análisis; si no lo hace, aparece el paso seleccionado.

Creación de filtros de coincidencia previa

Puede crear un filtro de coincidencia previa para que el archivo XMP limite la búsqueda de la información del evento que se desea analizar. El filtro de coincidencia previa identifica una cadena de texto seleccionado para limitar el proceso de selección de eventos, que se lleva a cabo mediante filtros de análisis. Si imaginamos el archivo de análisis como un embudo, el filtro de coincidencia previa es la boca del embudo y el filtro de análisis su extremo inferior.

Cuanto más completo sea el filtro de coincidencia previa, más eficaz será el proceso de análisis. Esto se debe a que la restricción de las categorías de coincidencia previa permite reducir el esfuerzo de procesamiento necesario para analizar eventos.

Por ejemplo, si desea analizar eventos de intentos de acceso, puede crear un filtro de coincidencia previa que busque el texto "inicio de sesión" y agregar los filtros de análisis correspondientes a dicho filtro de coincidencia previa.

Nota: La supresión de un filtro de coincidencia previa también elimina los filtros de análisis asociados.

Para crear filtros de coincidencia previa

1. Abra el Asistente del archivo de análisis y vaya al paso Asignar y analizar.
El asistente muestra los filtros de coincidencia previa existentes en la lista Filtros de coincidencia previa. Cada uno de ellos muestra el número de coincidencias previas con cualquier evento de ejemplo entre paréntesis situado junto a él.
2. Haga clic en Agregar una cadena de coincidencia previa en la parte superior de la lista Filtros de coincidencia previa o seleccione un filtro de coincidencia previa para editarlo.

Nota: Para seleccionar un filtro de coincidencia previa, introduzca los primeros caracteres de la cadena de coincidencia previa en el campo de búsqueda. Aparecerán todas aquellas cadenas de coincidencia previa que coincidan con los caracteres introducidos. Tras la búsqueda, no es posible utilizar las flechas de dirección entre los resultados de cadenas de coincidencia previa que aparezcan en pantalla.

3. Introduzca el texto que desea que busque el filtro en el campo de entrada Cadena de coincidencia previa.

Inmediatamente, aparecen todos los eventos de ejemplo que coinciden con el texto introducido, así como el número de eventos coincidentes detectados y analizados.

4. (Opcional) Haga clic en Agregar coincidencia previa en función de los eventos no coincidentes para mostrar todos los eventos de ejemplo no coincidentes.

En el área de eventos, aparecen todos los eventos de ejemplo no coincidentes para emplearlos como referencia al crear un nuevo filtro de coincidencia previa.

5. (Opcional) Agregue o edite más filtros de coincidencia previa según lo estime necesario.
6. Establezca el orden en el que desea que el proceso de análisis busque las coincidencias previas mediante las flechas de dirección junto a la lista Filtros de coincidencia previa. Si se establecen filtros que coinciden con más eventos en una posición más elevada de la lista de prioridad, se incrementa la eficacia del proceso de análisis.
7. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario de archivo de análisis; si no lo hace, aparece el paso seleccionado.

Creación de filtros de análisis

Puede crear un filtro de análisis para definir cómo analiza el archivo XMP los datos de eventos. Cada filtro de análisis está vinculado a un filtro de coincidencia previa. Tras la ubicación de una cadena de coincidencia previa, el proceso de análisis emplea los filtros de análisis vinculados a dicha coincidencia previa por orden para detectar la información especificada. El proceso de análisis muestra la primera coincidencia positiva que encuentra.

Al hacer clic en el botón Agregar un filtro de análisis en el paso de coincidencia y análisis del asistente de análisis de mensajes, se inicia el asistente del filtro de archivos de análisis. Para crear filtros de análisis eficaces, necesita conocer a fondo la sintaxis de las expresiones regulares.

Para crear filtros de análisis

1. Abra el asistente del filtro de archivos de análisis y escriba el nombre de un filtro y una descripción opcional en la página Detalles del filtro.
2. Haga clic en Agregar nuevo para añadir un valor de campo estático que desee mostrar en todos los eventos analizados por el filtro.

Aparece una fila de campo estático en la que se muestran las celdas de campo nuevo y valor nuevo.
3. Introduzca un valor en la celda de campo nuevo y en la celda de valor nuevo. La función de relleno automático reduce los nombres de campo de gramática de eventos comunes disponibles a medida que escribe en la celda de campo nuevo y le muestra un menú de opciones.
4. (Opcional) Repita los pasos 2 y 3 para agregar valores de campo estáticos según sea necesario.
5. Vaya al paso de expresión regular.

Se abre la ventana Prueba de la expresión de análisis, que muestra todas las expresiones regulares actuales. Justo debajo de la expresión regular está el panel Evento. Esta área muestra uno o más eventos de ejemplo si ha cargado eventos de ejemplo previamente. El asistente puede probar estos eventos con respecto a la expresión regular a medida que la crea.

6. Haga clic en Agregar o eliminar tokens de la biblioteca para mostrar una lista de las expresiones regulares predefinidas que puede agregar para emplearlas en el filtro actual. Seleccione los tokens que desea agregar y haga clic en Aceptar para añadirlos a la lista de tokens de análisis.

7. (Opcional) Haga clic en Nuevo token de expresión regular para crear un token de análisis e introduzca la sintaxis de la expresión regular en el panel Detalles del token. Ahora puede crear expresiones personalizadas para su entorno. Puede agregar un token personalizado a la biblioteca local mediante un clic en Agregar token seleccionado a la biblioteca en la parte superior del panel de tokens de análisis.

Nota: Cuando cree un token de fecha y hora nuevo, seleccione la casilla de verificación 'Tratar como un valor de fecha y hora' para introducir un formato para analizar el valor de tiempo. Este valor no afecta al formato de visualización.

8. Agregue instrucciones de expresiones regulares para el filtro en el campo de entrada Expresión regular. Puede arrastrar expresiones de la lista de tokens de análisis. También puede introducir o editar la expresión directamente en el campo de entrada Expresión regular.

Nota: La selección de un token en la lista de tokens de análisis muestra su sintaxis de expresiones regulares en el panel Detalles del token. Puede ver la asignación de tokens de análisis en una regla determinada para repetirla en otras reglas de análisis.

9. (Opcional) Seleccione la casilla de verificación Nombre dinámico/Pares de valores si los eventos de destino incluyen pares de claves que desea visualizar. Consulte "Análisis dinámico" para obtener más información.
10. (Opcional) Si desea emplear el análisis dinámico, introduzca una expresión de análisis dinámico en el campo de entrada de pares dinámicos. Por ejemplo, introduzca:

```
(_PAIR_KEY_)=(_PAIR_VALUE_);
```

Aparecen todos los pares separados por un signo igual y delimitados mediante un punto y coma. Puede introducir más expresiones para encontrar pares mostrados en otros formatos. Consulte Análisis dinámico para obtener más información.

11. Realice una vista previa de cómo el archivo analiza los eventos de ejemplo mediante los paneles Evento y Evento analizado. A medida que modifica la expresión regular del filtro de análisis, las partes analizadas del evento de ejemplo se resaltan con texto de color azul y los pares analizados dinámicamente aparecen en verde. Puede comprobar la eficacia del análisis.
12. (Opcional) Cambie de evento de ejemplo para realizar otra prueba mediante las flechas de avance y retroceso del panel Evento para desplazarse por los eventos de ejemplo disponibles.
13. Haga clic en Guardar y cerrar cuando esté satisfecho con la expresión regular. Puede emplear la opción Restablecer para devolver la expresión regular a su estado inicial.

El asistente del filtro de archivos de análisis se cierra y vuelve a aparecer el paso de asignación y análisis del asistente del archivo de análisis.

Más información:

[Análisis dinámico](#) (en la página 568)

[Tokens de análisis](#) (en la página 569)

[Adición de un token personalizado a la biblioteca](#) (en la página 573)

Análisis dinámico

Puede utilizar el análisis dinámico, que permite la visualización de varios pares nombre-valor sin alterar. Este análisis es distinto al análisis estático, que extrae valores y los establece en la Gramática de eventos comunes u otros campos predefinidos. El análisis dinámico es útil donde las aplicaciones o formatos registran datos de eventos en pares clave que desee que se muestre sin alterar, es decir, no analizado en los nombres de la Gramática de eventos comunes u otros valores. También mejora el rendimiento del análisis en los casos en los que sea aplicable.

La expresión regular que permite el análisis dinámico consta de cuatro elementos:

1. Un indicador de clave de par "(_PAIR_KEY_)".
2. Un indicador de valor de par "(_PAIR_VALUE_)".
3. Un separador clave-valor entre el par y el valor de clave.
4. Un separador de par entre toda la expresión y la siguiente expresión.

Los separadores que use deben coincidir con la estructura del origen de evento que está analizando. Si el origen de evento utiliza una coma como separador, la expresión regular debe hacerlo también.

ejemplo

```
(_PAIR_KEY_)=(_PAIR_VALUE_);
```

En este ejemplo el separador clave-valor es "=" y el separador de par es ";".

Esta expresión después de otras expresiones regulares permite que se ubique el archivo XMP y muestre los pares de clave que aparecen en los eventos analizados.

Tokens de análisis

Un token de análisis es una plantilla de expresión regular que puede emplear para crear filtros de análisis. CA Enterprise Log Manager incluye una biblioteca de tokens de análisis que contiene tokens de análisis predefinidos. Por ejemplo, el token `_IP_` define la expresión regular que analiza el formato de dirección IP habitual. Cuando desea que un filtro de análisis extraiga una dirección IP, puede insertar el token `_IP_` en el filtro en lugar de construir cada vez todo el lenguaje de la expresión regular.

También puede crear sus propios tokens de análisis personalizados y añadirlos a la biblioteca local, así como exportarlos para su empleo en otro entorno de CA Enterprise Log Manager. Si desea exportar un token personalizado, añádalo primero a la biblioteca. También puede importar tokens personalizados de otro entorno de CA Enterprise Log Manager para crear tokens de análisis en un entorno de prueba y, a continuación, desplazarlos a un entorno real.

Más información:

[Valores de tokens de fecha y hora](#) (en la página 570)

[Adición de un token personalizado a la biblioteca](#) (en la página 573)

[Supresión de un token personalizado de la biblioteca](#) (en la página 574)

[Importación de tokens de análisis](#) (en la página 575)

[Exportación de tokens de análisis](#) (en la página 576)

Valores de tokens de fecha y hora

CA Enterprise Log Manager admite varias opciones de sintaxis para tokens de análisis de fecha y hora. Puede emplear estas opciones, en formato de fecha y hora del archivo de análisis, para personalizar la apariencia de la marca de fecha y hora.

Cada token de fecha y hora consta de uno de los elementos siguientes:

- Un carácter ordinario (ni '%' ni un carácter de espacio en blanco), que se muestra tal y como se ha introducido: por ejemplo, dos puntos para separar valores de tiempo.
o
- Una especificación de conversión. Cada especificación de conversión consta de un carácter '%' seguido de un carácter de conversión que define la apariencia de la pantalla: por ejemplo, %m para indicar el mes.

CA Enterprise Log Manager admite las especificaciones de conversión siguientes:

%a o %A

Muestra el nombre del día de la semana local, de manera completa o abreviada. En Windows, esta especificación sólo está disponible en inglés estadounidense.

%b, %B o %h

Muestra el nombre del mes local, de manera completa o abreviada. En Windows, esta especificación sólo está disponible en inglés estadounidense.

%c

Muestra la fecha y hora locales.

%C

Muestra el número de siglo (0-99).

%d o %e

Muestra el día del mes (1-31).

%D

Muestra la fecha con formato americano: Mes/Día/Año, que equivale a la introducción de %m/%d/%y.

Nota: En Europa, se emplea la sintaxis %d/%m/%y. El formato correspondiente a la norma ISO 8601 es %Y-%m-%d.

%H

Muestra la hora en un reloj de 24 horas (0-23).

%I

Muestra la hora en un reloj de 12 horas (1-12).

%j

Muestra el número de día del año (1-366).

%m

Muestra el número de mes (1-12).

%M

Muestra el minuto (0-59).

%n

Introduce un espacio en blanco arbitrario.

%p

Muestra el equivalente local de AM o PM si existe.

%r

Muestra la hora del reloj de 12 horas: Hora:Minuto:Segundo AM/PM, que equivale a la introducción de %I:%M:%S %p. Si t_fmt_ampm está vacío en la sección LC_TIME local, entonces el comportamiento es indefinido.

%R

Muestra la hora del reloj de 24 horas: Hora:Minuto, que equivale a la introducción de %H:%M.

%S

Muestra el segundo (0-60 - 60 puede aparecer en el caso de segundos adicionales).

%t

Muestra un espacio en blanco arbitrario.

%T

Muestra la hora del reloj de 24 horas: Hora:Minuto:Segundo, que equivale a la introducción de %H:%M:%S.

%U

Muestra el número de semana. El domingo es el primer día de la semana (0-53). El primer domingo de enero es el primer día de la semana 1.

%w

Muestra el número de día de la semana (0-6), donde domingo = 0.

%W

Muestra el número de semana con el lunes como primer día de la semana (0-53). El primer lunes de enero es el primer día de la semana 1.

%x

Muestra la fecha mediante el formato de fecha local.

%X

Muestra la hora mediante el formato de hora local.

%y

Muestra el año del siglo actual (0-99). Cuando no se especifica un siglo, los valores del rango de 69 a 99 hacen referencia a años del siglo XX (1969-1999); los valores del rango de 00 a 68 hacen referencia a años del siglo XXI (2000-2068).

%Y

Muestra el año, incluido el siglo (por ejemplo, 1991).

%z

Muestra una especificación de zona horaria correspondiente a la norma RFC-822/ISO 8601. Esta especificación no está disponible en Windows.

El formato de token de fecha y hora de CA Enterprise Log Manager predeterminado es:

`%d/%b/%Y:%H:%M:%S %z`

Adición de un token personalizado a la biblioteca

Puede agregar tokens de análisis personalizados a la biblioteca de tokens para que estén disponibles para otros usuarios. Por ejemplo, si crea un token personalizado durante el proceso de creación de archivos de análisis de mensajes, y éste podría resultar útil para otros análisis, puede añadirlo a la biblioteca para volver a utilizarlo.

En el procedimiento siguiente, se presupone que agrega tokens durante la creación de filtros o archivos de análisis.

Para agregar un token de análisis personalizado a la biblioteca

1. Abra el asistente de análisis de mensajes y vaya al paso de coincidencia y análisis.
2. Abra el asistente de filtro de archivos de análisis y vaya al paso de expresión regular.
3. Haga clic en Nueva expresión regular para crear un token de análisis e introduzca la sintaxis de la expresión regular en el panel Detalles del token.
4. Seleccione el token de análisis nuevo y haga clic en Agregar token seleccionado a la biblioteca.

Aparecerá un cuadro de diálogo de confirmación.

5. Haga clic en Sí.
6. (Opcional) Haga clic en Agregar o eliminar tokens de la biblioteca para ver el token nuevo.

Aparece el cuadro de diálogo de la biblioteca de tokens de análisis, que muestra los tokens personalizados en negro y los tokens predefinidos en verde.

Supresión de un token personalizado de la biblioteca

Puede eliminar de la biblioteca de tokens aquellos tokens personalizados que resulten innecesarios o estén obsoletos. No se puede eliminar los tokens predefinidos.

Para suprimir tokens personalizados de la biblioteca

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Asignación y análisis.

Los botones de integración de productos aparecen en el panel de detalles.

3. Haga clic en Nueva regla de análisis de mensajes: 

Se abre el asistente para el archivo de análisis.

4. Vaya al paso de asignación y análisis.

5. Seleccione un filtro de coincidencia previa y haga clic en Editar o en Agregar un filtro de análisis en la parte superior de la lista Filtros de análisis.

Aparece el asistente de filtro de archivos de análisis.

6. Vaya al paso de expresión regular.

7. Haga clic en Agregar o eliminar tokens de la biblioteca.

Aparece el cuadro de diálogo de la biblioteca de tokens de análisis, que muestra los tokens personalizados en negro y los tokens predefinidos en verde.

8. Seleccione los tokens personalizados que desea eliminar y haga clic en Eliminar token seleccionado de la biblioteca.

Aparecerá un cuadro de diálogo de confirmación.

9. Haga clic en Sí y, a continuación, en Aceptar.

Importación de tokens de análisis

Por ejemplo, puede importar tokens de análisis para agregar tokens de análisis personalizados creados en otro servidor de gestión al servidor actual, de un entorno de prueba al entorno real.

Para importar tokens de análisis

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Asignación y análisis.

Los botones de integración de productos aparecen en el panel de detalles.

3. Haga clic en Nueva regla de análisis de mensajes: 

Se abre el asistente para el archivo de análisis.

4. Vaya al paso de asignación y análisis.

5. Seleccione un filtro de coincidencia previa y haga clic en Editar o en Agregar un filtro de análisis en la parte superior de la lista Filtros de análisis.

Aparece el asistente de filtro de archivos de análisis.

6. Vaya al paso de expresión regular.

7. Haga clic en Importar tokens de usuario en la parte superior del panel de tokens de análisis.

Aparecerá el cuadro de diálogo Importar archivo.

8. Busque el archivo de tokens (.tok) que desea importar y haga clic en Aceptar.

Aparecerá un cuadro de diálogo de confirmación.

9. Haga clic en Sí si desea importar el archivo, sobrescribiendo los demás tokens de usuario de la biblioteca.

Exportación de tokens de análisis

Puede exportar tokens de análisis añadidos a la biblioteca de tokens para trasladar los tokens de análisis creados en el servidor de gestión actual a otro servidor. Por ejemplo, puede trasladar los tokens personalizados de un entorno de prueba al entorno real.

Para exportar tokens de análisis

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Asignación y análisis.

Los botones de integración de productos aparecen en el panel de detalles.

3. Haga clic en Nueva regla de análisis de mensajes: 

Se abre el asistente para el archivo de análisis.

4. Vaya al paso de asignación y análisis.

5. Seleccione un filtro de coincidencia previa y haga clic en Editar o en Agregar un filtro de análisis en la parte superior de la lista Filtros de análisis.

Aparece el asistente de filtro de archivos de análisis.

6. Vaya al paso de expresión regular.

7. Haga clic en Exportar tokens de usuario en la parte superior del panel de tokens de análisis.

Aparecerá un cuadro de diálogo de ubicación de descarga.

8. Seleccione la ubicación donde desee guardar el archivo exportado y haga clic en Guardar.

El archivo exportado se guarda en la ubicación seleccionada.

Análisis del archivo XMP

Puede emplear la utilidad de análisis de mensajes para analizar el archivo nuevo o editado y determinar la eficacia del archivo de análisis en los eventos de ejemplo. El análisis le permite introducir modificaciones para mejorar la eficacia del archivo antes de guardarlo.

La utilidad analiza un archivo XMP con respecto al conjunto de eventos de ejemplo seleccionados a través del proceso siguiente:

1. Ubicación de todos los eventos que contienen las cadenas de coincidencia previa definidas en el archivo XMP. La utilidad ejecuta una búsqueda independiente para cada cadena de coincidencia previa, buscando todos los eventos que contiene dicha cadena.
2. Búsqueda del primer filtro de análisis de cada uno de los eventos de coincidencia previa que puede analizar el evento en tokens.

Para analizar archivos XMP

Abra el asistente de análisis y vaya al paso de análisis. El asistente muestra el número de coincidencias con los filtros y las cadenas de coincidencia previa. Cuantas más coincidencias obtenga, más eficaz será el archivo XMP nuevo o editado. Esto también le permite determinar si existe alguna información relevante que no se haya analizado.

El análisis de XMP puede procesarse durante cierto tiempo si tanto el archivo XMP como el número de eventos de ejemplo son grandes. Normalmente, no debería llevar más de un minuto. Puede cancelar este proceso si dura demasiado tiempo y volver a realizar el análisis con un número de eventos más reducido.

Cuando crea una regla nueva, se guarda como versión 1.0. Si, posteriormente, la edita, se almacena una copia independiente de la regla como una versión nueva. Puede visualizar versiones anteriores, así como aplicarlas y copiarlas según desee.

Creación de archivos de asignación de datos

Puede emplear el asistente de archivo de asignación para crear y editar archivos de asignación de datos que convierten los eventos nativos en eventos refinados mediante la asignación de pares de campos/valores o cadenas de texto analizado a archivos compatibles con la gramática de eventos comunes. El asistente de archivo de asignación le permite crear y editar varios tipos de asignaciones para lograr esto.

El proceso de creación o edición de un archivo de asignación de datos consta de los pasos siguientes:

1. Apertura del asistente de archivo de asignación.
2. Indicación de detalles sobre el archivo.
3. Ubicación y adición de eventos de ejemplo mediante archivos de análisis.
4. Establecimiento de asignaciones directas según sea necesario.
5. Establecimiento de asignaciones de función según sea necesario.
6. Establecimiento de asignaciones condicionales según sea necesario.
7. Establecimiento de asignaciones de bloque según sea necesario.

Nota: Puede establecer asignaciones directas o de función mediante asignaciones de bloque. Son una alternativa al establecimiento de asignaciones mediante los pasos 4 y 5.

8. Análisis y almacenamiento del archivo de asignación de datos finalizado.

Al crear un archivo de asignación de datos, debe tener en cuenta las prioridades de asignación de datos del propio archivo, así como los tipos de asignaciones individuales dentro del archivo. El archivo de asignación de datos finalizado comprueba la información de eventos en el orden de las pantallas de tipo de asignación (pasos 4-7 del asistente). Si existen tipos de asignaciones duplicados, el último valor que detecta el archivo de asignación de datos es el que se asigna.

Por ejemplo, si un archivo de asignación de datos encuentra una asignación directa para un valor de evento nativo determinado y, a continuación, una asignación condicional diferente para el mismo valor, el evento refinado empleará el resultado de la asignación condicional.

Las asignaciones duplicadas *pertenecientes* a un tipo de asignación determinado se gestionan de otro modo, en función del tipo:

- Asignaciones directas y de función: el archivo de asignación de datos emplea el último valor de coincidencia encontrado. Si se detecta una asignación de función duplicada, se activará la última función. Por ejemplo, puede establecer que una asignación duplicada active una segunda función si la primera no se ha podido encontrar o no ha funcionado como se esperaba.
- Asignaciones condicionales y de bloque: el archivo de asignación de datos aplica el primer valor encontrado y deja de buscar. Para mejorar el rendimiento, debe indicar más condiciones comunes en el archivo para ambos tipos de asignación.

En los procedimientos de tipos de asignaciones individuales, se incluye más información sobre las implicaciones de diseño del orden de asignación.

Más información

[Establecimiento de asignaciones de bloque](#) (en la página 589)

[Realización de análisis de asignaciones](#) (en la página 591)

Apertura del asistente para el archivo de asignación

Para crear un archivo de asignación de datos nuevo o editar uno existente, debe abrir el asistente para el archivo de asignación.

Para abrir el asistente para el archivo de asignación

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.
2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Asignación y análisis.

Los botones de integración de productos aparecen en el panel de detalles.

3. Haga clic en Nuevo archivo de asignación: 

Aparece el asistente para el archivo de asignación.

Al emplear el asistente:

- Haga clic en Guardar para guardar el archivo sin cerrar el asistente.
- Haga clic en Guardar y cerrar para guardar el archivo y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Más información

[Establecimiento de asignaciones de función de concatenación](#) (en la página 586)

[Establecimiento de asignaciones de bloque](#) (en la página 589)

[Realización de análisis de asignaciones](#) (en la página 591)

Provisión de detalles de archivos

Proporcione detalles de archivo para un archivo DM nuevo. Puede guardar un archivo de suscripción como archivo personalizado con un nombre diferente.

Para ofrecer detalles sobre archivos de asignación

1. Abra el asistente del archivo de asignación.
2. Introduzca un nombre para el archivo de asignación de datos. El nombre de archivo es obligatorio y no puede contener los caracteres siguientes: / \ : * ? " < > ^ ; ' , & { } [] o | .
3. Seleccione el nombre y la versión del archivo de análisis que desea emplear para analizar los eventos de muestra en la lista desplegable Archivo de análisis.

El campo de nombre del registro se rellena de forma automática con el nombre del archivo de análisis introducido.

4. (Opcional) Escriba una descripción.
5. (Opcional) Haga clic en Agregar producto en el área de información de soporte para introducir las versiones y el nombre de un producto como referencia.
6. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario del archivo de asignación; si no lo hace, aparece el paso seleccionado.

Ofrecimiento de eventos de ejemplo

Puede emplear al asistente de archivos de asignación para buscar eventos de ejemplo con el fin de utilizarlos en el análisis del archivo de asignación de datos. Puede buscar en el sistema de almacenamiento de registro de eventos u ofrecer eventos de ejemplo directamente desde un archivo de registro. Los eventos de ejemplo ofrecen una plantilla con la que se puede comprobar el resultado de la asignación en el paso final del asistente.

Para ofrecer eventos de ejemplo

1. Abra el asistente del archivo de asignación y vaya al paso de eventos de ejemplo.

Aparece la pantalla de eventos de ejemplo.

2. Seleccione el botón de opción Almacén de registro o Archivo de registro en el área de búsqueda de eventos de ejemplo.
3. Si selecciona Almacén de registros:
 - a. Seleccione el tipo de origen de evento de ejemplo que desee en el menú desplegable Columna de análisis. Seleccione `result_string` para los orígenes de eventos WMI, o `raw_event` para los orígenes de eventos syslog.
 - b. Seleccione la consulta que desea emplear para ofrecer eventos de ejemplo mediante el filtro de etiquetas de consulta y la lista de consultas.

Aparece la consulta, que muestra los eventos de ejemplos.

Nota: Puede emplear cualquier consulta disponible o personalizada para localizar eventos de ejemplo. Si pretende utilizar una consulta personalizada, le recomendamos que la cree y la pruebe antes de comenzar el proceso de diseño del archivo de asignación de datos.

4. Si selecciona Archivo de registro:
 - a. Busque el archivo de registro que desee y haga clic en Cargar.
Los eventos del archivo de registro aparecen en el panel Eventos de ejemplo.
Nota: El asistente asume que cada línea del archivo es un evento. No se admiten eventos de varias líneas.
 - b. Haga clic en Extraer campos dinámicos si el archivo de registro de ejemplo contiene valores de par dinámico que desea incluir en el ejemplo analizado.
5. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario del archivo de asignación; si no lo hace, aparece el paso seleccionado.

Más información:

[Análisis dinámico](#) (en la página 568)

Establecimiento de asignaciones directas

Las asignaciones directas establecen correspondencias unívocas entre un evento nativo y un único valor de evento refinado. Por lo tanto, es mejor utilizar las asignaciones directas únicamente para valores predeterminados o valores comunes que no se suelen modificar, como el campo `ideal_model`.

Una asignación puede establecerse para derivar un valor de evento refinado de los modos siguientes:

Valor de texto

Establece un texto específico para un determinado campo de la gramática de eventos comunes. Este valor aparece cada vez que se asigna un evento adecuado. Por ejemplo, al establecer el campo `ideal_model` de la gramática de eventos comunes como "Cortafuegos", el campo `ideal_model` muestra "Cortafuegos" en todas las reglas que contienen esa asignación.

Valor de campo

Establece un campo de evento sin formato cuyo contenido se incluye para una gramática de eventos comunes o un archivo analizado determinados. Un valor de campo se distingue de un valor de texto porque el valor va precedido del símbolo del dólar: \$. Por ejemplo, si se establece el campo `event_logname` de la gramática de eventos comunes como "\$Registro", todos los eventos asignados mostrarán el texto que aparezca en el campo de registro del evento nativo.

Para establecer asignaciones directas

1. Abra el asistente de archivos de asignación, introduzca un nombre y seleccione un nombre de registro para el archivo de asignación; a continuación, vaya al paso de asignaciones directas.

Aparece la pantalla Asignaciones directas, en la que aparecen las asignaciones actuales o predeterminadas. La columna de nombre muestra el nombre del campo analizado o de gramática de eventos comunes. La columna de valor muestra un valor de texto o un valor de campo.

Nota: Seleccione un archivo de análisis en el paso de proporción de eventos de ejemplo para que aparezcan los valores de campo analizados.

2. Haga clic en Agregar asignación directa para agregar una nueva entrada de asignación en la parte inferior de la tabla y, a continuación, selecciónela o seleccione una asignación directa actual para editarla.

Las asignaciones directas del archivo, si las tiene, aparecen en el área de detalles de asignación.

3. Seleccione un campo de la gramática de eventos comunes o un campo de eventos analizados, si hay alguno disponible, para realizar la asignación en el menú desplegable Campo. Cuando empieza a escribir, la característica de relleno automático limita la lista de campos disponibles de la gramática de eventos comunes.
4. Introduzca un valor nuevo en el campo de entrada Agregar valor y haga clic en Agregar asignación directa junto a él. Coloque un símbolo "\$" antes del valor para indicar que se trata de un valor de campo y no un valor de texto. El valor aparece en el área de campos seleccionados.
5. (Opcional) Puede introducir múltiples asignaciones directas para un único campo mediante las flechas hacia arriba y hacia abajo para establecer el orden en el que las colocará el archivo DM. El evento refinado muestra la última asignación directa localizada por el archivo de asignación de datos.
Nota: La adición de múltiples valores reduce el rendimiento de la asignación, así que debe tener cuidado a la hora de emplear esta función.
6. (Opcional) Utilice el control de cambio para desplazar los valores no necesarios al área de campos disponibles para evitar que se tengan en cuenta en la asignación actual.
7. Cuando haya agregado todas las asignaciones directas deseadas, haga clic en la flecha correspondiente para ir al paso del asistente que desee completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario del archivo de asignación; si no lo hace, aparece el paso seleccionado.

Establecimiento de asignaciones de función

Las asignaciones de función vinculan un campo de gramática de eventos comunes al valor mediante una función empleada para definir la información de evento refinado que aparece en el evento refinado. Todas las asignaciones de función constan de un nombre de campo de gramática de eventos comunes, un valor de campo predefinido o de clase y la función.

Por ejemplo, una asignación de función puede concatenar una serie de valores de eventos nativos a un único campo de la gramática de eventos comunes mediante la función de concatenación.

Si hay asignaciones de función duplicadas, el archivo DM emplea la última que encuentra. Puede establecer que una asignación duplicada active una segunda función si la primera no se ha podido encontrar o no ha funcionado como se esperaba.

Para establecer asignaciones de función

1. Abra el asistente de archivos de asignación, introduzca un nombre y seleccione un nombre de registro para el archivo de asignación; a continuación, vaya al paso de asignaciones de función.

Aparece la pantalla Asignaciones de función, en la que aparecen las asignaciones actuales o predeterminadas. La columna de nombre muestra un campo analizado o de gramática de eventos comunes; la columna de función muestra la función de enlace actual; y la columna de valor muestra un valor de texto o de campo.

Nota: Seleccione un archivo de análisis en el paso de proporción de detalles del archivo para que aparezcan los valores de campo analizados.

2. Haga clic en Agregar asignación de función para añadir una nueva entrada de asignación o seleccione una asignación actual para editarla.

La entrada de asignación aparece en el panel Detalles de la asignación.

3. Seleccione un campo de gramática de eventos comunes para realizar la asignación en el menú desplegable Campo. Cuando empieza a escribir, la característica de relleno automático limita la lista de campos disponibles de la gramática de eventos comunes.
4. Seleccione una función que desee emplear en la asignación en el menú desplegable Función.

Nota: La función de concatenación funciona de un modo distinto de las demás, ya que se deben especificar múltiples valores de destino. Si desea obtener más información, consulte Establecimiento de asignaciones de función de concatenación.

5. Introduzca un valor de destino para la asignación en el campo de entrada Agregar valor y haga clic en el botón Agregar valor situado junto a él. Puede colocar un símbolo "\$" antes del valor para indicar que se trata de un valor de campo y no un valor específico.

El valor aparece en el área de campos seleccionados.

6. (Opcional) Puede introducir múltiples asignaciones para un único campo mediante las flechas hacia arriba y hacia abajo para establecer el orden en el que las colocará el archivo DM.

Nota: La adición de múltiples valores reduce el rendimiento de la asignación, así que sólo debe emplear asignaciones de función independientes si es necesario.

7. (Opcional) Utilice el control de cambio para desplazar los valores no necesarios al área de campos disponibles para evitar que se tengan en cuenta en la asignación actual.
8. Cuando haya agregado todas las asignaciones de función deseadas, haga clic en la flecha correspondiente para ir al paso del asistente que desee completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario del archivo de asignación; si no lo hace, aparece el paso seleccionado.

Establecimiento de asignaciones de función de concatenación

Las asignaciones de función de concatenación son un tipo de asignaciones de función. Al contrario de lo que ocurre con otras asignaciones de función, que especifican un valor o campo de destino, la función de concatenación especifica múltiples destinos de asignación que concatena en un campo de gramática de eventos comunes.

Puede emplear el asistente de asignación de datos para crear asignaciones de función de concatenación. Como las asignaciones de concatenación son diferentes de las demás asignaciones de función, el procedimiento para crearlas es ligeramente distinto.

Para establecer asignaciones de función de concatenación

1. Abra el asistente de archivos de asignación, introduzca un nombre y seleccione un nombre de registro para el archivo de asignación; a continuación, vaya al paso de asignaciones de función.

Aparece la pantalla Asignaciones de función, en la que aparecen las asignaciones actuales o predeterminadas. La columna de nombre muestra un campo de gramática de eventos comunes; la columna de función muestra la función de enlace actual; y la columna de valor muestra un valor de texto o de campo.

2. Haga clic en Agregar asignación de función para añadir una nueva entrada de asignación.

La entrada de asignación aparece en el panel Detalles de la asignación.

3. Seleccione un campo de gramática de eventos comunes para realizar la asignación en el menú desplegable Campo.

4. Seleccione la función de concatenación en el menú desplegable Función.

Aparecen los campos Formato y Valor.

Nota: El valor de la función de concatenación se muestra como {...} en el panel Asignaciones de función. Esto significa que existe un conjunto de valores en lugar de un solo valor.

5. (Opcional) Introduzca un especificador en el campo Formato para controlar la colocación de los campos de destino. El especificador de formato, %, indica una posición de campo. Cualquier valor distinto de %s hace que se considere que los datos de soporte estáticos se incluyen en el campo del colector de la tabla final. Por ejemplo, para separar dos campos de destino mediante dos puntos, introduzca "%s:%s" en el campo Formato.
6. Haga clic en Agregar valor concatenado en el área de valores concatenados para agregar un par de valor/entrada de destino.
7. Introduzca un valor en el campo de entrada Agregar valor y haga clic en Agregar valor.
El valor aparece en el área de campos seleccionados.
8. Repita los pasos 6 y 7 para agregar más valores para su concatenación. Debe agregar al menos dos valores de destino.
9. Cuando haya agregado todas las asignaciones de concatenación deseadas, haga clic en la flecha correspondiente para ir al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario de archivo de asignación; si no lo hace, aparece el paso seleccionado.

Establecimiento de asignaciones condicionales

Las asignaciones condicionales vinculan un campo de gramática de eventos comunes a diferentes resultados posibles, de manera que puede establecer valores predeterminados y condicionales para un campo determinado. Por ejemplo, podría emplear asignaciones condicionales para asignar valores de ejecución correcta o incorrecta, o para identificar orígenes de eventos por nombre o grupo.

Las asignaciones condicionales asignan un valor predeterminado y uno o más valores condicionales a un determinado campo de gramática de eventos comunes. Puede establecer calificaciones para cada valor condicional. Si un evento coincide con esas calificaciones, el valor condicional correspondiente se asigna al campo seleccionado. De otro modo, el campo de evento refinado muestra el valor predeterminado.

Si hay asignaciones condicionales duplicadas, el archivo DM empleará la primera que encuentre y no tendrá en cuenta las demás asignaciones. Para mejorar el rendimiento, debe colocar las condiciones más comunes en primer lugar.

Nota: La asignación condicional independiente es más lenta que la asignación de bloque. Le recomendamos que sólo la utilice en caso necesario.

Para establecer asignaciones condicionales

1. Abra el asistente de archivos de asignación, introduzca un nombre y seleccione un nombre de registro para el archivo de asignación; a continuación, vaya al paso de asignaciones condicionales.

Aparece la pantalla Asignaciones condicionales, que muestra todas las asignaciones predeterminadas actuales. La columna de campo muestra el nombre del campo analizado o de gramática de eventos comunes y la columna de valor muestra el valor predeterminado actual.

Nota: Seleccione un archivo de análisis en el paso de proporción de detalles del archivo para que aparezcan los valores de campo analizados.

2. Haga clic en Agregar asignación condicional en la lista Asignaciones de campo condicionales y seleccione la fila nueva.

Aparece el panel Detalles de la asignación, que muestra la lista desplegable Campo y el control de cambio de valor.

3. Seleccione el campo de gramática de eventos comunes para realizar la asignación en el menú Campo. Cuando empieza a escribir, la característica de relleno automático limita la lista de campos disponibles de la gramática de eventos comunes.
4. Introduzca la asignación predeterminada deseada en el campo de entrada Agregar valor y haga clic en Agregar valor para mostrarlo en el panel Campos seleccionados. Puede eliminar valores no deseados desplazándolos al panel Campos disponibles.
5. Haga clic en Agregar valor condicional en la lista Valores condicionales. Aparece un valor nuevo.
6. Seleccione el texto de valor nueva para resaltarlo y cámbiele el nombre. El nombre nuevo se muestra en la lista y aparece el cuadro diálogo de filtros en el panel de detalles.
7. Cree un filtro para definir el valor condicional. Por ejemplo, puede crear uno o más filtros para vincular el campo `event_source_address` a direcciones IP, identificando orígenes de eventos con un grupo geográfico o de otra empresa.
8. Cuando haya agregado todas las asignaciones condicionales deseadas, haga clic en la flecha correspondiente para ir al paso del asistente que desee completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario del archivo de asignación; si no lo hace, aparece el paso seleccionado.

Establecimiento de asignaciones de bloque

Las asignaciones de bloque vinculan una condición seleccionada a una determinada serie de asignaciones, lo que le permite crear una cascada de asignaciones activadas por dicha condición. Una asignación de bloque determinada puede emplear cualquier combinación de asignaciones de función o directas. Ambos tipos de asignación de bloque interna funcionan del mismo modo que lo harían para asignaciones independientes.

Puede crear tantos bloques como necesite para un único archivo de asignación. Cada uno incluye un nombre y una condición.

Si hay asignaciones duplicadas en un bloque determinado, el archivo de asignación de datos empleará la primera que encuentre y no tendrá en cuenta las demás asignaciones. Para mejorar el rendimiento, debe colocar las condiciones más comunes en primer lugar.

Para establecer asignaciones de bloque

1. Abra el asistente de archivos de asignación, introduzca un nombre y seleccione un nombre de registro para el archivo de asignación; a continuación, vaya al paso de asignaciones de bloque.

Aparece la pantalla Asignaciones de bloque, que muestra todas las asignaciones de bloque actuales.
2. Haga clic en Agregar asignación de bloque en el panel Asignaciones de bloque.

Aparece un bloque nuevo en la lista de asignaciones de bloque.
3. Seleccione el texto del bloque nuevo.

Se abre el panel de definición del bloque, que muestra el Paso 1. Definir una condición
4. Introduzca un nombre de bloque y cree un filtro para definir la condición de dicho bloque. Por ejemplo, puede definir event_result como "S", en cuyo caso, las asignaciones de bloque se activarán cuando se detecte una situación correcta del proceso de evento.
5. Haga clic en la barra del paso 2 e introduzca las asignaciones directas que desee a través del mismo proceso que el del paso de asignación independiente.
6. Haga clic en la barra del paso 3 e introduzca las asignaciones de función que desee a través del mismo proceso que el del paso de asignación independiente.
7. Cuando haya agregado todas las asignaciones de bloque deseadas, haga clic en la flecha correspondiente para ir al paso del asistente que desee completar a continuación, o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el archivo nuevo aparece en la carpeta de usuario de archivo de asignación; si no lo hace, aparece el paso seleccionado.

Más información

[Uso de filtros avanzados](#) (en la página 509)

Realización de análisis de asignaciones

Puede emplear el asistente de asignaciones para analizar un archivo de asignación de datos. De este modo, podrá realizar pruebas y modificaciones para aumentar la eficacia del archivo de asignación. Los eventos de ejemplo se prueban con respecto al archivo de asignación de datos y se validan con la gramática de eventos comunes.

Para realizar análisis de asignaciones, vaya al paso de análisis de asignaciones del asistente de archivo de asignación. El asistente muestra una tabla que indica el resultado del análisis de los eventos de ejemplo introducidos en el paso de evento de ejemplo.

El archivo de asignación de datos completado guarda las asignaciones y tiene en cuenta la información del evento en el orden indicado por las pantallas de tipo de asignación (pasos 4-7 del asistente). Si existen asignaciones duplicadas, el último valor que detecta el archivo de asignación de datos es el que se asigna. Por ejemplo, si un archivo de asignación de datos encuentra una asignación directa para un valor de evento nativo determinado y, a continuación, una asignación condicional diferente para el mismo valor, el evento refinado mostrará el resultado de la asignación condicional. En los procedimientos de tipos de asignaciones individuales, se incluye más información sobre las implicaciones de diseño del orden de asignación.

Cuando crea una regla nueva, se guarda como versión 1.0. Si, posteriormente, la edita, se almacena una copia independiente de la regla como una versión nueva. Puede visualizar versiones anteriores, así como aplicarlas y copiarlas según desee.

Tareas de reglas de transferencia de eventos

Las reglas de transferencia de eventos le permiten seleccionar eventos de CA Enterprise Log Manager para transferirlos a escuchas remotas en sistemas o aplicaciones externos. Puede emplear las reglas de transferencia para identificar los eventos que desea transferir, establecer cuándo se van a transmitir y controlar cómo se reciben. Cuando un evento entrante coincide con un filtro de regla de transferencia, CA Enterprise Log Manager crea una copia del evento y la transfiere. El evento sigue estando registrado en el almacén de registro de eventos.

Las tareas de reglas de transferencia de eventos se llevan a cabo en el área de recopilación de registros de la interfaz de CA Enterprise Log Manager. Puede crear, editar y eliminar reglas de transferencia de eventos. También puede importar o exportar dichas reglas.

Más información:

[Creación de reglas de transferencia de eventos](#) (en la página 592)

Creación de reglas de transferencia de eventos

Puede emplear reglas de transferencia de eventos para enviar eventos de CA Enterprise Log Manager a aplicaciones externas. Por ejemplo, puede enviar eventos a CA NSM mediante syslog. Las reglas de transferencia de eventos le permiten establecer criterios para los eventos que desea transferir, así como establecer uno o más receptores.

El proceso de creación de reglas de transferencia de eventos mediante el asistente de reglas de transferencia consta de los pasos siguientes:

1. Apertura del asistente de reglas de transferencia.
2. Definición de un nombre y una descripción opcional de la regla.
3. Creación de filtros simples y avanzados para identificar los eventos que se desean transferir.
4. Definición de atributos de reglas, como el destino de la transferencia y los campos de la gramática de eventos comunes, que se incluirán en el evento transferido.

Más información:

[Asignación de un nombre a la regla de transferencia](#) (en la página 594)

[Creación de un filtro de evento simple](#) (en la página 594)

[Creación de filtros de eventos avanzados](#) (en la página 597)

[Uso de filtros avanzados](#) (en la página 533)

[Definición de atributos de reglas de transferencia](#) (en la página 598)

Apertura del asistente de reglas de transferencia

Para crear una regla de transferencia o editar una existente, abra el asistente de reglas de transferencia.

Para abrir el asistente de reglas de transferencia

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.

2. Seleccione la carpeta Reglas de transferencia.

Los botones de reglas de transferencia aparecen en el panel de detalles.

3. Haga clic en Nueva regla de transferencia: 

Se abre el asistente de reglas de transferencia.

Al emplear el asistente:

- Haga clic en Guardar para guardar el archivo de la regla sin cerrar el asistente.
- Haga clic en Guardar y Cerrar para guardar el archivo de la regla y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Asignación de un nombre a la regla de transferencia

Debe asignar un nombre a cada regla de transferencia. También puede introducir información descriptiva como referencia.

Para nombrar una regla de transferencia

1. Abra el asistente de reglas de transferencia.
2. Introduzca un nombre para la regla. El nombre es obligatorio y no puede contener los caracteres siguientes: / \ : * ? < > ; ' , & { } [] . o | .
3. (Opcional) Introduzca información descriptiva sobre la regla como referencia.
4. Vaya al paso de filtrado.

Creación de un filtro de evento simple

Puede crear filtros simples que le permitirán establecer parámetros de búsqueda de campos de la gramática de eventos comunes. Por ejemplo, puede configurar el campo Modelo ideal como "Gestión de contenido" para identificar todos los eventos que tengan ese valor en el campo de la gramática de eventos comunes de Modelo ideal. Son numerosas las funciones que utilizan filtros simples, por ejemplo, las consultas, las reglas de resumen y supresión, y las reglas de transferencia de eventos.

Para crear un filtro simple

1. Seleccione la casilla de verificación de Modelo ideal, o bien los campos Evento que desee definir, y seleccione un valor en la lista desplegable o introduzca el valor en el campo de entrada de texto.
2. (Opcional) Si va a crear un filtro de consulta, seleccione las casillas de verificación de los campos Origen, Destino o Agente, e introduzca el valor deseado en el campo de entrada de texto.
3. Repita los pasos 1 a 2 para agregar otros filtros simples.
4. Haga clic en Guardar cuando haya agregado todos los filtros simples que desee.

Más información

[Uso de filtros avanzados](#) (en la página 509)

[Creación de filtros de eventos avanzados](#) (en la página 597)

Uso de filtros avanzados

Puede usar filtros avanzados basados en SQL para calificar cualquier función que consulte el almacenamiento de registro de eventos, incluida la limitación de consultas o la personalización de filtros rápidos. La interfaz Filtros avanzados le ayuda a crear la sintaxis apropiada para los filtros proporcionando un formulario para introducir columnas, operadores y valores lógicos en función de los requisitos de filtrado.

Nota: Esta sección contienen una breve descripción general de los términos SQL usados en los filtros avanzados. Para aprovechar al máximo el potencial de los filtros avanzados, debe conocer a fondo SQL y la gramática de eventos comunes.

Los siguientes términos SQL unen varias instrucciones de filtros:

And

Muestra la información del evento si *todos* los términos unidos son verdaderos.

Or

Muestra la información del evento si *alguno* de los términos unidos es verdadero.

Having

Restringe las condiciones de la instrucción SQL principal añadiendo una instrucción de calificación. Por ejemplo, puede definir un filtro avanzado para eventos de determinados hosts y añadir una instrucción "having" para mostrar sólo los eventos de esos host que presenten un nivel de severidad específico.

Los filtros avanzados utilizan los siguientes operadores SQL para crear las condiciones básicas:

Operadores relacionales

Incluye la información del evento si la columna tiene la relación apropiada con el valor introducido. Dispone de los siguientes operadores relacionales:

- Equal to
- Not Equal to
- Less than
- Greater than
- Less than or equal to
- Greater than or equal to

Por ejemplo, si usa *Greater than*, incluiría la información del evento de la columna elegida si su valor fuera mayor que el valor especificado.

Like

Incluye la información del evento si la columna contiene un patrón que haya introducido, usando % para definir el patrón deseado. Por ejemplo, L% devolvería cualquier valor que empezara por L, y %L% devolvería cualquier valor que tuviera una L, pero no como primera o última letra.

Not like

Incluye la información del evento si la columna no contiene el patrón especificado.

In set

Incluye la información del evento si la columna contiene uno o varios valores del conjunto entrecomillado introducido. Debe separar con comas los diferentes valores del conjunto.

Not in set

Incluye la información del evento si la columna no contiene uno o varios valores del conjunto entrecomillado introducido. Debe separar con comas los diferentes valores del conjunto.

Matches

Incluye cualquier información del evento que coincida con uno o más de los caracteres introducidos, de manera que puede buscar por palabras clave.

Keyed

Incluye cualquier información del evento que se haya definido como valor clave durante la configuración del servidor de informes. Puede emplear valores clave para definir la relevancia empresarial u otros grupos organizativos.

Not Keyed

Incluye cualquier información del evento que no se haya definido como valor clave durante la configuración del servidor de informes. Puede emplear valores clave para definir la relevancia empresarial u otros grupos organizativos.

Creación de filtros de eventos avanzados

Los filtros avanzados se usan en muchas funciones, incluida la creación de consultas, la planificación de informes y los filtros locales y globales.

Para crear filtros avanzados

1. Haga clic en Nuevo filtro de evento.
La primera fila de la tabla de filtros de eventos se activa y sus columnas Lógica y Operador se rellenan con los valores predeterminados "And" y "Equal to" respectivamente.
2. (Opcional) Haga clic en la celda Lógica y cambie el valor lógico según sea necesario.
3. Haga clic en la celda Columna y seleccione la columna de información del evento deseado en el menú desplegable.
4. Haga clic en la celda Operador y seleccione el operador deseado en el menú desplegable.
5. Haga clic en la celda Valor e introduzca el valor deseado.
6. (Opcional) Haga clic en las celdas de paréntesis de apertura y cierre e introduzca el número de paréntesis que necesita.
7. (Opcional) Repita los pasos de 1 a 6 según sea necesario para agregar más instrucciones de filtros.
8. Haga clic en Guardar cuando haya introducido todas las instrucciones de filtro que desee.

Más información

[Uso de filtros avanzados](#) (en la página 509)

[Programación de tareas de informes](#) (en la página 506)

Definición de atributos de reglas de transferencia

Defina los atributos necesarios para una regla de transferencia, incluidos los puntos de salida de transferencias, los campos de la gramática de eventos comunes presentes en el evento transferido, así como la configuración de destino.

Para definir los atributos de las reglas

1. Abra el asistente de reglas de transferencia y vaya al paso de atributos de política.
2. Defina las acciones de las reglas de transferencia en el área de acciones:
 - a. Seleccione una funcionalidad de syslog y una severidad de syslog en las listas desplegables correspondientes. Cualquier evento transferido por la regla incluye los atributos de syslog definidos.
3. Defina información sobre la transmisión de eventos de CA Enterprise Log Manager en el área de información general:
 - a. Seleccione si desea enviar los eventos identificados por la regla antes o después de la supresión y el resumen:
 - Si decide hacerlo antes, todos los eventos entrantes se verifican con respecto a los filtros de reglas de transferencia.
 - Si decide hacerlo después, los eventos refinados serán los únicos que se verificarán con respecto a los filtros de reglas de transferencia; los eventos suprimidos no se transfieren y los eventos resumidos sólo se transfieren como resumidos, no con los detalles previos al resumen.

Nota: Si decide hacerlo antes, tendrá una mayor repercusión en el rendimiento del sistema, ya que los eventos no están refinados.

 - a. Seleccione los campos de la gramática de eventos comunes que desea mostrar en el evento transmitido. Si no selecciona un campo de la gramática de eventos comunes, sólo se envía el valor del evento sin formato. Si selecciona *algún* campo de la gramática de eventos comunes, seleccione también `raw_event` para transferir el evento sin formato.
4. Defina la información de destino de la transferencia en el área de destino:
 - a. Haga clic en Agregar destino para crear una fila de destino.
 - b. Haga clic en la columna Host para agregar un nombre de host de destino o una dirección IP. La dirección IP puede ser IPv4 o IPv6.
 - c. Haga clic en la celda de la columna Puerto para agregar el número de puerto que escucha la aplicación de destino.

- d. Haga clic en el texto de la columna Protocolo para seleccionar TCP o UDP para definir el protocolo de transmisión que desea emplear.
 - e. Repita los pasos a-d para agregar más destinos a continuación.
5. Haga clic en Guardar o en Guardar y cerrar.

La regla nueva aparece en la subcarpeta Usuario de la carpeta Reglas de transferencia.

Acerca de los eventos de syslog reenviados

El tamaño máximo para el paquete de syslog (incluidos los campos PRI, Encabezado, Etiqueta y Contenido) es de 1.024 bytes, por lo que es posible que el evento reenviado no pueda incluir todas las parejas valor-nombre de gramática de eventos comunes que el usuario haya especificado.

Cuando sea necesario, CA Enterprise Log Manager trunca el valor del mensaje para mantener la longitud por debajo de 1.024 bytes. Si la regla especifica que se incluyan campos de la gramática de eventos comunes en el evento de syslog generado, el campo Contenido del evento de syslog generado contiene las parejas valor-nombre especificadas de la gramática de eventos comunes.

Las parejas valor-nombre tienen el formato *CEG_field_name:field_value* del evento que coincidió con la regla de filtro simple. La cadena “nulo” designa un valor nulo del campo de la gramática de eventos comunes. Estos campos de la gramática de eventos comunes aparecen en el orden especificado en la regla de reenvío.

El orden de los campos de la gramática de eventos comunes especificado en la regla de reenvío es significativo. CA Enterprise Log Manager puede truncar la porción del valor especificado, pero no truncará ningún nombre de campo de la gramática de eventos comunes. Si CA Enterprise Log Manager no puede adaptar el siguiente nombre completo de campo de la gramática de eventos comunes ni los dos puntos y, al menos, un byte del valor asociado, se finaliza el campo de contenido de syslog con la anterior pareja valor-nombre de la gramática de eventos comunes.

Edición de reglas de transferencia

Puede editar reglas de transferencia.

Para editar una regla de transferencia

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la carpeta Reglas de transferencia y haga clic en la carpeta que contiene el archivo que desee editar.
3. Seleccione la regla que desea editar y haga clic en el icono de edición de reglas de transferencia.

Aparece el asistente de reglas de transferencia que muestra la regla seleccionada.

4. Modifique la regla como desee y haga clic en Guardar y cerrar.

La regla aparece en la lista correspondiente como versión nueva de la regla editada.

Supresión de reglas de transferencia

Puede eliminar reglas de transferencias no necesarias.

Para suprimir una regla de transferencia

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la carpeta Reglas de transferencia y haga clic en la carpeta que contiene el archivo que desee suprimir.
3. Seleccione la regla que desea eliminar y haga clic en el icono de supresión de reglas de transferencia. Se selecciona de forma predeterminada la versión actual. Puede seleccionar una versión anterior para su eliminación en la lista desplegable Versión del panel de detalles.

Aparecerá un cuadro de diálogo de confirmación.

4. Haga clic en Sí.

La regla eliminada se quita de la lista correspondiente.

Importación de reglas de transferencia

Puede importar reglas de transferencia, ya que puede mover las reglas de un entorno a otro. Por ejemplo, podría importar reglas creadas en un entorno de prueba a un entorno real.

Para importar una regla de transferencia

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Seleccione la carpeta Reglas de transferencia.
Los botones de reglas de transferencia aparecen en el panel de detalles.
3. Haga clic en Importar regla de transferencia.
Aparece el cuadro de diálogo de importación de archivo.
4. Busque la regla que desea importar y haga clic en Aceptar.
Aparece el asistente de reglas de transferencia, que indica los detalles de la regla seleccionada.
5. Modifique la regla como desee y haga clic en Guardar y cerrar. Si la regla importada tiene el mismo nombre que otra regla que ya se encuentra en la base de datos de gestión, deberá cambiarle el nombre.
La regla importada aparece en la carpeta de usuario de reglas de transferencia de eventos.

Exportación de reglas de transferencia

Puede exportar reglas de transferencia, ya que puede mover las reglas de un entorno a otro. Por ejemplo, podría exportar reglas creadas en un entorno de prueba a un entorno real.

Para exportar una regla de transferencia

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la carpeta Reglas de transferencia y haga clic en la carpeta que contiene el archivo que desee exportar.
3. Seleccione la regla que desea exportar y, a continuación, haga clic en Exportar regla de transferencia. Se selecciona de forma predeterminada la versión actual. Puede seleccionar una versión anterior para su exportación en la lista desplegable Versión del panel de detalles.

Aparece un cuadro de diálogo de ubicación de exportación.

4. Introduzca o busque la ubicación en la que desea almacenar la regla exportada y haga clic en Guardar.

Aparece un cuadro de diálogo de confirmación de exportación correcta.

5. Haga clic en OK.

La regla se exporta.

Nota: Si examina la regla exportada, los valores de Funcionalidad y Severidad sólo se muestran de forma numérica. Puede emplear la interfaz del asistente para determinar las descripciones de texto asociadas a estos valores.

Capítulo 16: Integraciones y conectores

Esta sección contiene los siguientes temas:

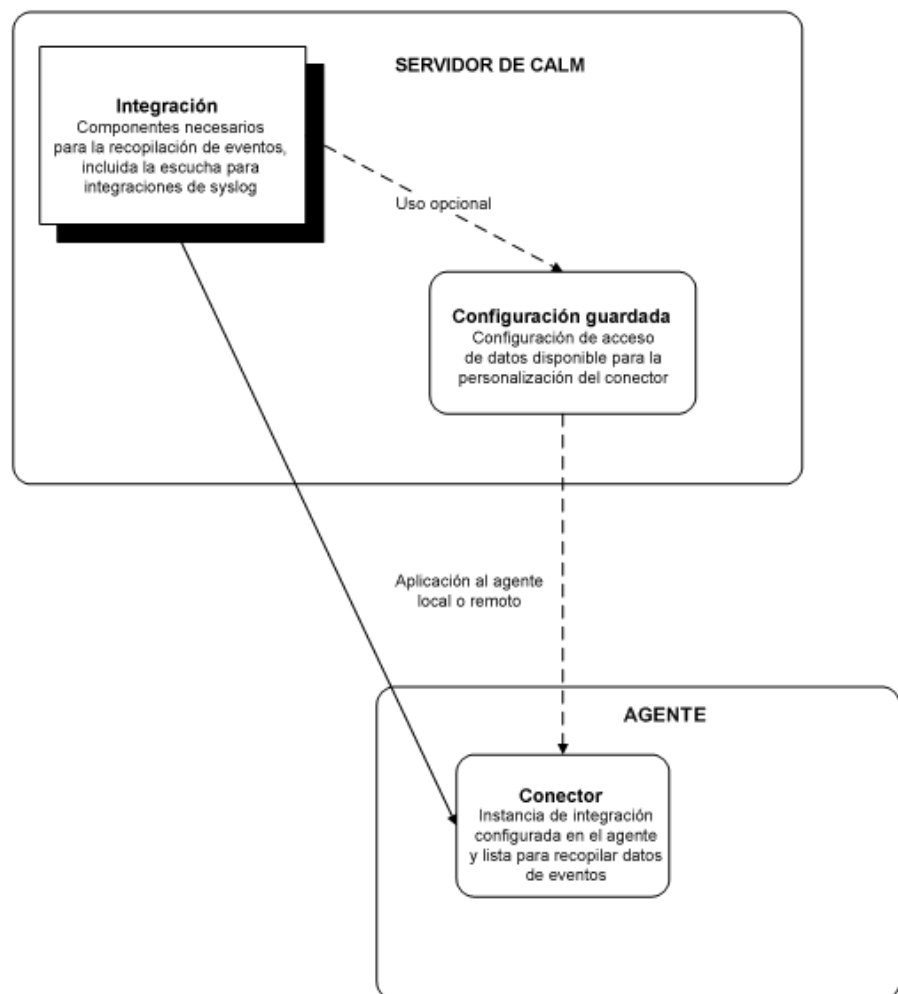
- [Tareas de integración y conectores](#) (en la página 603)
- [Creación de una integración](#) (en la página 605)
- [Creación de escuchas de syslog](#) (en la página 613)
- [Creación de versiones de integraciones nuevas](#) (en la página 620)
- [Eliminación de integraciones](#) (en la página 621)
- [Exportación e importación de definiciones de integraciones](#) (en la página 621)
- [Creación de conectores](#) (en la página 623)
- [Visualización de conectores](#) (en la página 627)
- [Vista de guía del conector](#) (en la página 628)
- [Edición de conectores](#) (en la página 629)
- [Acerca de las configuraciones guardadas](#) (en la página 629)
- [Creación de configuraciones guardadas](#) (en la página 630)
- [Configuración de conectores de forma masiva](#) (en la página 631)
- [Actualización de varias configuraciones de conectores](#) (en la página 637)

Tareas de integración y conectores

Una integración es una plantilla para conectores. Incluye todos los componentes necesarios para recopilar la información de eventos de un tipo de origen determinado: un sensor de registro, archivos XMP y de asignación de datos, así como reglas de supresión opcionales. Las integraciones las ofrece CA. Los usuarios también pueden crear sus propias integraciones.

Puede crear una integración personalizada o modificar la copia de una integración predefinida. También puede crear sus propios archivos XMP o de asignación de datos para emplearlos en integraciones personalizadas, así como integraciones almacenadas que contienen información específica de acceso a datos.

Tras analizar un evento y crear la integración necesaria, puede crear un conector mediante las configuraciones almacenadas y aplicarlo a un agente, tal y como se muestra en la ilustración siguiente:



Más información

[Exportación e importación de definiciones de integraciones](#) (en la página 621)

[Acerca de las configuraciones guardadas](#) (en la página 629)

[Visualización de conectores](#) (en la página 627)

[Edición de conectores](#) (en la página 629)

Creación de una integración

Puede emplear el asistente de integración para crear o editar integraciones, que sirven como plantillas para los conectores configurados que recopilan o reciben eventos del entorno.

Puede crear integraciones de varios tipos e incluir conectores WMI y ODBC, que recopilan de forma activa eventos del tipo especificado. También puede crear integraciones de syslog, que reciben los eventos de forma pasiva. Las integraciones de syslog pueden recibir eventos de más de un origen. Por lo tanto, el proceso de creación de un conector y una integración de syslog es ligeramente diferente.

Para aprovechar al máximo esta función avanzada, debe poseer un profundo conocimiento de los orígenes de eventos de en su entorno, así como de los tipos de comunicación. Además, debe poseer un profundo conocimiento de la sintaxis de expresión regular, la gramática de eventos comunes, los archivos DM y XMP y de cómo analizan eventos.

La creación y la integración constan de los pasos siguientes:

1. Apertura del asistente de integración.
2. Adición de componentes de integración.
3. Selección de reglas de supresión.
4. Selección de reglas de resumen.
5. Establecimiento de configuraciones predeterminadas. Este paso no se aplica a las integraciones de syslog.

También puede crear una integración de usuario personalizada mediante la copia de una integración de suscripción.

Más información:

[Adición de componentes de integración](#) (en la página 607)

[Aplicación de reglas de resumen y supresión](#) (en la página 608)

[Establecimiento de configuraciones predeterminadas](#) (en la página 609)

Apertura del asistente de integración

Para crear una integración nueva o editar una existente, abra el asistente de integración.

Para abrir el asistente de integración

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.
2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Integraciones.

Los botones de integración aparecen en el panel de detalles.

3. Haga clic en Nueva integración: 

Aparece el asistente de integración.

Al emplear el asistente:

- Haga clic en Guardar para guardar el archivo sin cerrar el asistente.
- Haga clic en Guardar y cerrar para guardar el archivo y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Más información:

[Adición de componentes de integración](#) (en la página 607)

Adición de componentes de integración

Cuando puede crear una integración, establece los detalles de la integración, como los sensores de registro, los archivos XMP y los archivos DM empleados para recopilar eventos.

Para agregar componentes de integración

1. Abra el asistente de integración.
2. Introduzca un nombre para la integración nueva.
3. Seleccione los componentes de integración requeridos en las listas desplegables:

Sensor

Define el sensor de registro que emplea la integración para leer eventos del origen de eventos.

Ayudante de la configuración

Define el binario del ayudante que emplea la integración para conectarse al sistema de almacenamiento de registro de eventos. La mayor parte de las integraciones no requiere un ayudante de configuración.

Plataforma

Hace referencia al sistema operativo que el agente de integración puede ejecutar, *no* al sistema operativo de la aplicación que la integración debe supervisar. El asistente selecciona de forma automática el sistema operativo según los ajustes de la ayuda de configuración y del sensor.

4. Introduzca una descripción de la integración.
5. Utilice los controles de cambio para seleccionar los archivos XMP y de asignación de datos que desea que emplee la integración para refinar eventos.
6. Si fuera necesario, introduzca el nombre del campo nativo que contiene la información de eventos sin formato que desea que analice la integración en el campo de entrada 'Campos de destino'. Algunos tipos de eventos contienen la información de eventos sin formato en un determinado campo, que requiere que la integración se dirija a dicho campo. Por ejemplo, para los eventos de registro de eventos de NT, este campo se llama "Mensaje".
7. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la integración nueva aparece en la lista de la carpeta del usuario; si no es así, aparece el paso que haya seleccionado.

Aplicación de reglas de resumen y supresión

Puede aplicar reglas de resumen y supresión a una integración para agilizar el refinamiento de eventos. Cuando la integración se configura como conector, las reglas de resumen y supresión se aplican antes de enviarse al almacén de registro de eventos. La comprobación de resumen y supresión se añade a la comprobación de resumen y supresión realizada en el almacén de registro de eventos.

Por ejemplo, puede aplicar una regla de supresión para que los eventos de Windows no deseados no se envíen a un agente WMI. El tráfico de red se reduce y estos eventos nunca llegan al almacén de registro de eventos.

Importante: Debería crear y utilizar las reglas de supresión con cuidado, ya que evitan el inicio de sesión y la aparición de determinados eventos nativos por completo. Le recomendamos que compruebe las reglas de supresión en un entorno de prueba antes de implementarlas.

Para aplicar reglas de resumen y supresión

1. Abra el asistente de integración y vaya al paso de reglas de supresión o al paso de reglas de resumen.
2. (Opcional) Introduzca datos en el campo de patrón de reglas para buscar las reglas disponibles. A medida que escribe, se muestran las reglas que coinciden con el texto introducido.
3. Seleccione las reglas deseadas mediante el control de cambio.
4. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la integración nueva aparece en la lista de la carpeta del usuario; si no es así, aparece el paso que haya seleccionado.

Más información:

[Tareas de reglas de resumen y supresión](#) (en la página 528)

[Adición de componentes de integración](#) (en la página 607)

[Establecimiento de configuraciones predeterminadas](#) (en la página 609)

[Establecimiento de configuraciones del registro de archivos](#) (en la página 610)

Establecimiento de configuraciones predeterminadas

Puede controlar la configuración de acceso a los datos de la integración mediante configuraciones predeterminadas. Por ejemplo, puede establecer el controlador de dominios para que se conecte para realizar comunicaciones WMI.

Este paso no se aplica al crear una integración de syslog, ya que estas integraciones heredan los valores de configuración de la escucha de syslog.

Para establecer configuraciones predeterminadas

1. Abra el asistente de integración y vaya al paso de configuraciones predeterminadas.
2. Complete los campos necesarios.
3. (Opcional) Haga clic en el botón Ocultar situado junto a una configuración predeterminada para ocultarla durante la creación de un conector. Las configuraciones ocultas no estarán visibles para el usuario al crear un conector basado en esta integración. Por lo tanto, puede definir configuraciones predeterminadas que no se puedan cambiar cuando la integración se emplee para implementar un conector.
4. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.
Si hace clic en Guardar y cerrar, la integración nueva aparece en la lista de la carpeta del usuario; si no es así, aparece el paso que haya seleccionado.

Más información:

[Adición de componentes de integración](#) (en la página 607)

Establecimiento de configuraciones del registro de archivos

Puede controlar la configuración del acceso a los datos de las integraciones mediante el sensor del registro de archivos. Puede emplear la configuración predeterminada ofrecida por CA para la mayoría de los objetivos de recopilación de eventos, pero es posible que desee alterar esta configuración para las integraciones personalizadas.

Para establecer configuraciones del registro de archivos

1. Abra el asistente de integración, seleccione el tipo de sensor de registro de archivos y vaya al paso de configuraciones predeterminadas.
2. Defina o modifique la tasa de retención de la integración:

UpdateAnchorRate

Define el umbral, en eventos, en el que se crea un valor de retención. Si se interrumpe el procesamiento de eventos, el agente consulta el último valor de retención para reiniciar el procesamiento. La definición de una tasa de retención inferior reduce las posibilidades de que se pierdan eventos, pero afecta al rendimiento, ya que el valor de retención se crea más a menudo. La definición de una tasa de retención mayor aumenta la carga de trabajo, ya que muchos eventos se tendrán que volver a procesar en caso de que se interrumpa el procesamiento.

Predeterminado: 4

Leer desde el inicio

Controla si el agente comenzará a leer el archivo desde el principio si se interrumpe el procesamiento de eventos. Si la casilla de verificación no se selecciona, el agente reiniciará la lectura de eventos empleando la tasa de retención. Si se selecciona la casilla de verificación, el sensor leerá el archivo de registro desde el principio al implementar un conector por primera vez. Según el tamaño de la base de datos y el intervalo de generación de eventos, el sensor de registro de CA Enterprise Log Manager puede tardar varios minutos en sincronizarse con los eventos en tiempo real.

3. Defina o edite los valores de configuración siguientes para el origen de eventos de destino:

Directorio de almacenamiento de archivos

Define la ruta en la que se guarda el archivo de registro tras la rotación. El directorio de archivo y el nombre del directorio no pueden ser iguales.

Máscara de archivos

Establece una cadena de texto empleada para identificar el archivo de registro del origen de evento. La máscara de archivos puede emplear caracteres comodín. Por ejemplo, para identificar un archivo de registro denominado "mensajes.txt", puede introducir la máscara *mensajes**.

Tipo de rotación de archivos

Establece la integración que se corresponde con el tipo de rotación de archivos empleado por el producto desde el que recibe eventos. Este producto define el tipo de rotación real. Las integraciones de CA Enterprise Log Manager admiten los ajustes siguientes:

- NewFile: se utiliza cuando el destino de la integración se rota mediante una utilidad como logrotate.
- FileSize: se utiliza cuando el destino de la integración se basa en un umbral de tamaño predefinido.
- FileAge: se utiliza cuando el destino de la integración se basa en un período de tiempo predefinido. La actualización suele producirse alrededor de la medianoche.

Nombre de directorio

Define la ruta del archivo de registro del origen de evento.

Delimitador de evento

Define la expresión regular que separa las entradas de registro individuales en un archivo de registro con varias líneas. Cada vez que el sensor de registro encuentra el delimitador especificado, comienza a leer nuevos eventos. Esto permite que CA Enterprise Log Manager reciba varias entradas de eventos desde un solo archivo de registro. Por ejemplo, si cada entrada del archivo de registro contiene una marca de hora/fecha única, podrá utilizar la expresión regular como delimitador para ese formato de hora.

4. (Opcional) Para agregar más valores de origen de evento, haga clic en

Repetir: 

Aparece otro conjunto de campos de valores de configuración que le permiten introducir valores para la recopilación de eventos desde un origen de evento diferente.

5. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la integración nueva aparece en la lista de la carpeta del usuario; si no es así, aparece el paso que haya seleccionado.

Creación de escuchas de syslog

Puede emplear el asistente de escucha para crear o editar escuchas de syslog. La escucha controla el modo en que los eventos de syslog se enrutan hacia el servidor de CA Enterprise Log Manager.

Nota: Puede emplear la escucha de syslog de suscripción (predefinida) para casi todos sus objetivos. Algunos usuarios pueden desear ajustar su recepción de syslog mediante escuchas personalizadas, y estas instrucciones se incluyen para esos propósitos.

Para aprovechar al máximo esta función avanzada, debe poseer un profundo conocimiento de los orígenes de eventos de syslog en su entorno.

La creación y la integración constan de los pasos siguientes:

1. Apertura del asistente de escucha.
2. Adición de componentes.
3. Selección de reglas de supresión.
4. Selección de reglas de resumen.
5. Establecimiento de configuraciones predeterminadas.

Más información:

[Apertura del asistente de escucha](#) (en la página 614)

[Adición de componentes de escucha](#) (en la página 615)

[Establecimiento de configuraciones predeterminadas](#) (en la página 617)

[Aplicación de reglas de resumen y supresión](#) (en la página 616)

[Adición de zonas horarias a syslog](#) (en la página 619)

Apertura del asistente de escucha

Para crear una escucha de syslog nueva o editar una existente, abra el asistente de escucha.

Para abrir el asistente de escucha

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la flecha situada junto a la carpeta Biblioteca de refinamiento de eventos para expandirla y, a continuación, seleccione la carpeta Escuchas.

Los botones de integración aparecen en el panel de detalles.

3. Haga clic en Nueva escucha: 

Aparece el asistente de escucha.

Al emplear el asistente:

- Haga clic en Guardar para guardar el archivo sin cerrar el asistente.
- Haga clic en Guardar y Cerrar para guardar el archivo y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Adición de componentes de escucha

Para crear una escucha de syslog, defina detalles como una ayuda de configuración y un nombre.

Para agregar componentes de escucha

1. Abra el asistente de escucha.
2. Introduzca un nombre para la escucha nueva.
3. (Opcional) Seleccione el componente siguiente en la lista desplegable:

Ayudante de la configuración

Define el binario del ayudante que emplea la integración para conectarse al sistema de almacenamiento de registro de eventos. La mayor parte de las integraciones no requiere un ayudante de configuración.

Nota: El tipo de sensor de una escucha es siempre syslog.

4. (Opcional) Introduzca una descripción para la ayuda.
5. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la integración nueva aparece en la lista de la carpeta del usuario; si no es así, aparece el paso que haya seleccionado.

Aplicación de reglas de resumen y supresión

Puede aplicar reglas de resumen y supresión a una escucha de syslog con el fin de agilizar el refinamiento de eventos. Cuando la escucha se configura con un conector, los eventos entrantes se verifican con respecto a cualquier regla de resumen y supresión aplicada antes de enviarse a CA Enterprise Log Manager.

Por ejemplo, si desea crear una escucha para recibir sólo eventos de CA Access Control, puede aplicar la regla de acceso correcto a los archivos de CA Access Control. Esto le permite evitar un procesamiento excesivo, ya que sólo se utilizan las reglas necesarias para verificar los eventos entrantes.

Importante: Cree y utilice las reglas de supresión con cuidado, ya que evitan por completo el inicio de sesión y la aparición de determinados eventos nativos. Le recomendamos que compruebe las reglas de supresión en un entorno de prueba antes de implementarlas.

Para aplicar reglas de resumen o supresión

1. Abra el asistente de escucha y vaya al paso Reglas de supresión o al paso Reglas de resumen.
2. (Opcional) Introduzca datos en el campo de entrada de patrón de reglas para buscar las reglas disponibles. A medida que escribe, se muestran las reglas que se ajustan a los datos introducidos.
3. Seleccione las reglas que desee mediante el control de cambio.
4. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la escucha nueva aparece en la lista de la carpeta del usuario; si no es así, aparece el paso que haya seleccionado.

Establecimiento de configuraciones predeterminadas

Puede controlar la configuración de acceso a los datos de la escucha de syslog mediante configuraciones predeterminadas. Por ejemplo, puede establecer host de confianza o puertos de comunicación predeterminados.

Para establecer configuraciones predeterminadas

1. Abra el asistente de escucha y vaya al paso de configuraciones predeterminadas.
2. Modifique o añada los valores deseados, incluidos los siguientes:

Orden de eventos

Garantiza que los eventos se envían al almacén de registro de eventos en el mismo orden en el que se reciben. Si se desactiva el orden de eventos, el orden podrá modificarse si unos eventos se analizan y se envían más rápido que otros. La activación del orden de eventos puede afectar al rendimiento mediante una ralentización del procesamiento y el envío de eventos.

Recuento de subprocesos por cola

Define el número de subprocesos en procesamiento de cada protocolo. El empleo de varios subprocesos del procesamiento agiliza el procesamiento si se desactiva el orden de eventos. Si el orden de eventos está activado, el recuento de subprocesos no tendrá ningún efecto. El empleo de múltiples subprocesos puede afectar al rendimiento.

Tamaño de la cola

Define el tamaño de la cola, en número de eventos, para la información de eventos entrantes. La cola se emplea para procesar y enviar eventos. Si el búfer se llena, no se pueden recibir más eventos hasta que los eventos procesados no dejen espacio.

Puertos

Establece los puertos que emplea la escucha para recibir eventos mediante UDP o TCP. Si especifica varios puertos, el servicio trata de conectarse con cada uno por turnos. Los puertos predeterminados de syslog ya están establecidos. Si enruta eventos de syslog hacia otros puertos, debe establecer los puertos de recepción de CA Enterprise Log Manager del modo correspondiente.

Importante: Si el agente se ejecuta como un usuario no-root en un sistema UNIX, debe modificar los puertos de escucha de syslog para que tengan números de puerto superiores a 1024. En este caso, el puerto UDP 514 (valor predeterminado) no se abre y no se recopila ningún evento de syslog.

Host de confianza

Define direcciones IP de confianza para IPv4 o IPv6; sólo se aceptan comunicaciones de host de confianza. Si no especifica un host de confianza, se aceptan eventos de todos los orígenes de eventos de syslog disponibles. Debe introducir la dirección IP exacta tal y como figura en el campo event_source_address para host de confianza. No puede emplear comodines ni direcciones de subred.

Zonas horarias

Le permite agregar zonas horarias en equipos de origen de evento syslog. syslog no suele registrar la hora. Identifique los sistemas de origen mediante la dirección IP completa y la zona horaria para recibir y ajustar eventos de orígenes de syslog que se encuentren en una zona horaria diferente de la del servidor de CA Enterprise Log Manager. No realice una lista de orígenes de syslog en la misma zona horaria que la del servidor.

3. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la escucha nueva aparece en la lista de la carpeta del usuario; si no es así, aparece el paso que haya seleccionado.

Adición de zonas horarias a syslog

Agregue una zona horaria o más equipos de origen de eventos de syslog para recibir y ajustar de forma correcta los eventos de los orígenes de syslog que se encuentren en una zona horaria diferente de la del servidor de CA Enterprise Log Manager.

Puede agregar una zona horaria a syslog al crear una integración, al configurar un conector o al crear una configuración guardada.

Nota: Al agregar una zona horaria a un entorno en el que se emplea el horario de verano, asegúrese de que existe una zona horaria equivalente en el sistema del host de agente. Sin ella, la zona horaria de syslog no podrá procesar el cambio al horario de verano y los eventos se mostrarán con una indicación de tiempo errónea durante el período del horario de verano.

Para agregar zonas horarias a syslog

1. Acceda a la interfaz de zonas horarias de syslog de una de estas maneras:
 - Abra la integración de syslog a la que desea agregar zonas horarias y vaya al paso de configuración predeterminada.
 - Abra el conector de syslog al que desea agregar zonas horarias y vaya al paso de configuración de conector.
 - Abra la configuración guardada a la que desea agregar zonas horarias.Aparece la interfaz de zonas horarias de syslog.
2. Haga clic en Crear carpeta en la parte superior del área de zonas horarias.
Aparece una nueva carpeta de zona horaria en el área de listas y se muestra una lista desplegable de zonas horarias en el panel derecho.
3. Seleccione una zona horaria en la lista desplegable.
La zona seleccionada aparece junto a la carpeta.
4. Haga clic en la flecha situada junto a la carpeta.
La carpeta se expande y muestra un único equipo de origen de evento sin título para esa zona horaria.
5. Seleccione el icono del equipo.
Aparece el campo de introducción de la dirección IP.
6. Introduzca una dirección IP.
La dirección aparece junto al icono del equipo a medida que la introduce.

7. (Opcional) Para agregar más equipos de origen de evento, seleccione un origen de evento existente y haga clic en Agregar elemento.
La carpeta se cierra. Ábrala para mostrar un nuevo equipo de origen de evento sin título. Vaya al paso 6.
8. (Opcional) Para agregar más zonas horarias, haga clic en Crear carpeta.
Aparece una nueva carpeta de zona horaria sin título. Vaya al paso 3.
9. Cuando haya creado todas las carpetas de zonas horarias y los elementos de dirección de origen de evento deseados, haga clic en Guardar.

Más información:

[Establecimiento de configuraciones de conectores](#) (en la página 626)

[Creación de configuraciones guardadas](#) (en la página 630)

Creación de versiones de integraciones nuevas

Puede crear una versión nueva de una integración existente creada por el usuario (personalizada).

Para crear versiones de integraciones nuevas

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.
2. Expanda las carpetas Biblioteca de refinamiento de eventos e Integraciones y navegue hasta la carpeta de usuario que contenga la integración que desee.
3. Seleccione la integración de usuario y haga clic en Crear nueva versión.
4. Aparece el asistente de integración nueva y muestra los detalles de la integración seleccionada.
5. Realice los cambios deseados y haga clic en Guardar y cerrar.
La nueva versión de integración aparece en la lista.

Eliminación de integraciones

Puede eliminar integraciones personalizadas. No puede eliminar las integraciones de suscripción.

Para eliminar integraciones personalizadas

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.
2. Expanda las carpetas Biblioteca de refinamiento de eventos e Integraciones y navegue hasta la carpeta de usuario que contenga la integración que desee suprimir.
3. Haga clic en la integración que desea eliminar de la lista.
4. Haga clic en Suprimir en la parte superior de la lista.
Aparecerá un cuadro de diálogo de confirmación.
5. Haga clic en Sí.
La integración se elimina de la lista.

Exportación e importación de definiciones de integraciones

Puede exportar e importar detalles de integraciones para usarlos en otros servidores de gestión. Esto permite transferir integraciones personalizadas correctas entre entornos de CA Enterprise Log Manager, o de un entorno de prueba a otro real.

Más información

[Importación de definiciones de integraciones](#) (en la página 622)

[Exportación de definiciones de integraciones](#) (en la página 623)

Importación de definiciones de integraciones

Puede importar archivos XML de definición de integraciones para su uso en el servidor de gestión local.

Para importar detalles de integraciones

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la estructura de árbol de la carpeta Recopilación de registros.
2. Expanda la carpeta de integraciones y vaya a la subcarpeta donde desee importar una integración.
3. Haga clic en Importar integración.
Se abre un cuadro de diálogo de importación de archivo.
4. Introduzca o vaya a la ubicación del archivo que quiera importar y haga clic en Aceptar.
Los archivos de consulta se importan en la carpeta actual y aparece un cuadro de diálogo de confirmación.
5. Haga clic en Aceptar.

Exportación de definiciones de integraciones

Puede exportar detalles de integraciones para usarlos en otros servidores de gestión. La exportación se guarda como un archivo XML.

Para exportar detalles de integraciones

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la estructura de árbol de la carpeta Recopilación de registros.
2. Expanda la carpeta de integraciones y vaya a la subcarpeta que contiene la integración que desea exportar.
3. Haga clic en Exportar integraciones.
Aparece un cuadro de diálogo de descarga.
4. Introduzca o vaya a la ubicación en la que quiera guardar los archivos de exportación XML y haga clic en Guardar.
Los archivos de consulta se guardan en la ubicación elegida y aparece un cuadro de diálogo de confirmación.
5. Haga clic en Aceptar.

Creación de conectores

Puede crear un conector que recopile los eventos desde un sistema operativo o un dispositivo específico de su entorno. Utilice una integración o una escucha como plantilla para crear un conector mediante el nuevo asistente de conector. Cada conector nuevo se aplica a un agente del entorno.

Puede crear conectores de varios tipos, incluidas integraciones WMI y ODBC, que recopilan de forma activa eventos del tipo especificado. También puede crear conectores de syslog, que reciben los eventos de forma pasiva. A diferencia de los demás tipos, los conectores de syslog pueden recibir eventos desde más de un origen. Por lo tanto, el proceso de creación de un conector de syslog es ligeramente diferente.

El proceso de creación de un conector consta de los pasos siguientes:

1. Apertura del asistente de conector.
2. Adición de detalles del conector, incluida la selección de una escucha para los conectores de syslog.
3. Aplicación de las reglas de supresión.
4. Aplicación de las reglas de resumen.
5. Establecimiento de las configuraciones del conector.

Más información:

[Apertura del asistente de conector](#) (en la página 624)

[Adición de detalles de conectores](#) (en la página 625)

[Aplicación de reglas de resumen y supresión](#) (en la página 626)

[Establecimiento de configuraciones de conectores](#) (en la página 626)

Apertura del asistente de conector

Para crear un conector nuevo o editar uno existente, debe abrir el asistente de conector.

Para abrir el asistente de conector

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la lista de la carpeta Recopilación de registros.
2. Expanda la carpeta Explorador de agentes y seleccione el grupo de agentes en el que desea agregar o editar un conector.
Aparecen los agentes que pertenecen al grupo que ha seleccionado.
3. Seleccione el agente en el que desea agregar o editar un conector.
Los botones de gestión de agentes aparecen en el panel de detalles.

4. Haga clic en Nuevo conector: 

Aparece el asistente de conector.

Al emplear el asistente:

- Haga clic en Guardar para guardar el archivo sin cerrar el asistente.
- Haga clic en Guardar y Cerrar para guardar el archivo y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Adición de detalles de conectores

Puede agregar un nombre y una descripción para identificar el conector. También debe seleccionar la integración que desea emplear como plantilla para el conector.

Para agregar detalles de conectores

1. Abra el asistente de diseño de conector.

El asistente se abre y muestra la plataforma y la versión de la plataforma del agente actual en la parte superior de la pantalla.

2. Escriba un nombre para el conector.
3. Seleccione el botón de opción Escucha si desea crear un conector de syslog o seleccione el botón de opción Integración para elegir otro tipo.
4. Seleccione la integración que desea emplear como plantilla. La lista desplegable Integración muestra todas las integraciones disponibles para la versión actual de la plataforma y el tipo de origen del evento.
5. (Opcional) Seleccione Omitir comprobación de versión de plataforma para realizar integraciones para *todas* las versiones de la plataforma de agente disponibles en la lista desplegable Integración.
6. Escriba una descripción para el conector.
7. Vaya al paso que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el conector aparece en la lista de conectores.

Aplicación de reglas de resumen y supresión

Al crear o editar un conector, puede seleccionar las reglas de resumen y supresión que se aplicarán a los eventos gestionados por el conector. Todas las reglas de resumen o supresión que añada se aplicarán antes de que los eventos se transmitan al servidor de CA Enterprise Log Manager.

Para aplicar reglas de resumen o supresión

1. Abra el asistente de diseño de conector y vaya al paso Aplicar reglas de supresión o al paso Reglas de resumen.
Aparece una lista con las reglas de supresión de seguridad disponibles.
2. (Opcional) Introduzca datos en el campo de entrada de patrón de reglas para buscar las reglas disponibles. A medida que escribe, se muestran las reglas que se ajustan a los datos introducidos.
3. Seleccione las reglas que desea aplicar mediante el control de cambio.
4. Vaya al paso que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, el conector aparece en la lista de conectores.

Establecimiento de configuraciones de conectores

Al crear o editar conectores, puede establecer configuraciones individuales que determinan el modo en que el conector recibe y transmite eventos. Puede establecer las configuraciones de cada conector o emplear configuraciones almacenadas.

Las configuraciones guardadas son recopilaciones de configuraciones de acceso a datos que puede reutilizar. Puede aplicar las configuraciones guardadas a múltiples conectores.

Para establecer configuraciones de conectores

1. Abra el asistente de diseño de conector y vaya al paso de configuración de conectores.
2. Si ha seleccionado el sensor de registro/escucha de syslog, seleccione las integraciones que desea que emplee el conector.

3. Seleccione la configuración almacenada que desee en la lista desplegable o cambie los valores de configuración visualizados. Los conectores heredan los ajustes de configuración de la integración o la escucha en el caso de los conectores de syslog.
4. (Opcional) Haga clic en el vínculo Ayuda para visualizar la guía de conectores de la integración seleccionada. La guía mostrada ofrece información detallada.
5. Haga clic en Guardar y cerrar.
El conector aparece en la lista de conectores.

Visualización de conectores

Puede abrir la lista de conectores de cada agente para ver y editar conectores vinculados a dicho agente.

Para visualizar conectores

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la lista de la carpeta Recopilación de registros.
2. Expanda la carpeta Explorador de agentes y la del grupo de agentes para mostrar los agentes individuales
3. Seleccione el agente en el que se ha implementado el conector que desea visualizar.
4. Haga clic en Ver conectores: 
Aparece la lista de conectores de agente, que muestra los conectores implementados en el agente seleccionado.

Vista de guía del conector

Puede ver una guía que contenga la información de configuración y establecimiento de cada tipo de conector de CA Enterprise Log Manager. La guía cuenta con instrucciones sobre cómo configurar el producto de destino y el conector en sí mismo para recibir eventos.

También contiene información de referencia como los nombres de registros de conectores y los tipos de eventos que el conector transmite a CA Enterprise Log Manager.

Para ver una guía del conector

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.
2. Expanda las carpetas Biblioteca de refinamiento de eventos, Integraciones y Suscripción para visualizar las integraciones individuales.
3. Seleccione la integración que desee usar para crear un conector.
Aparecerán los detalles de integración en el panel derecho.
4. Haga clic en el vínculo de ayuda de color azul justo encima del nombre de integración.

La guía del conector para la integración aparecerá en una nueva ventana del explorador.

Edición de conectores

Puede editar un conector existente. La edición de un conector crea una versión nueva.

Para editar conectores

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Expanda la carpeta Explorador de agentes y la del grupo de agentes para mostrar los agentes individuales
3. Seleccione el agente en el que se ha implementado el conector que desea visualizar.

4. Haga clic en Ver conectores: 

Aparece la lista de conectores de agente, que muestra los conectores implementados en el agente seleccionado.

5. Haga clic en Editar junto al conector que desea editar.

Se abre el asistente de conector y muestra el conector seleccionado.

6. Realice los cambios deseados y haga clic en Guardar y cerrar.

El conector editado aparece en la lista.

Acerca de las configuraciones guardadas

Una configuración guardada es una recopilación reutilizable de ajustes que permite que un conector recopile eventos de un dispositivo o de un origen de registros. Puede emplear configuraciones guardadas para permitir un grado de personalización sin necesidad de crear una integración totalmente nueva.

Las configuraciones se diferencian según el tipo de integración. Por ejemplo, puede guardar host de confianza para un conector syslog, o información de contacto de servidor WMI para un conector WMI.

Las configuraciones guardadas le permiten retener esta información agrupada y aplicarla a múltiples conectores. Como cada configuración guardada se asocia a una integración en particular, sólo puede emplear una configuración guardada en conectores que empleen dicha integración.

Más información

[Creación de configuraciones guardadas](#) (en la página 630)

[Tareas de integración y conectores](#) (en la página 603)

Creación de configuraciones guardadas

Puede crear configuraciones guardadas asociándolas a integraciones específicas.

Para crear configuraciones guardadas

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Abra la carpeta Biblioteca de refinamiento de eventos y vaya a la integración en la que desea crear una configuración guardada.

En el panel de detalles, aparecen los detalles de la integración.

3. Haga clic en Configuraciones guardadas: 

Aparece la lista de configuraciones guardadas.

4. Haga clic en Nuevo.

Aparece el cuadro de diálogo Configuración guardada, que muestra los valores de configuración predeterminados de la integración seleccionada.

5. Introduzca los valores de configuración deseados y haga clic en Guardar y cerrar.

Aparece un mensaje de confirmación.

6. Haga clic en Aceptar.

La configuración guardada aparece en la lista.

Configuración de conectores de forma masiva

Puede configurar orígenes de recopilación de eventos mediante la creación de múltiples conectores de forma masiva. Puede crear múltiples conectores al mismo tiempo mediante las mismas integraciones, así como implementarlos en varios agentes del entorno.

El proceso de configuración incluye la selección de orígenes de eventos, la aplicación de reglas de supresión, la aplicación de reglas de resumen y el establecimiento de la configuración del conector. Antes de poder aprovechar las ventajas de esta función, cree una lista de información de identificación, como nombres de host y direcciones IP, para los orígenes de eventos que desea configurar. La lista debe tener un formato de valores separados por comas (.csv).

El proceso de configuración de orígenes de recopilación mediante el asistente de implementación del conector masivo consta de los pasos siguientes:

1. Apertura del asistente de implementación del conector masivo
2. Selección de información detallada del origen
3. Aplicación de las reglas de supresión
4. Aplicación de reglas de resumen
5. Configuración de ajustes del conector
6. Selección de agentes y orígenes de asignación

Más información:

[Apertura del asistente de configuración de orígenes de recopilación](#) (en la página 632)

[Selección de detalles del origen](#) (en la página 633)

[Aplicación de reglas de supresión](#) (en la página 634)

[Aplicación de reglas de resumen](#) (en la página 634)

[Configuración del conector](#) (en la página 635)

[Selección de agentes y asignación de orígenes](#) (en la página 636)

Apertura del asistente de configuración de orígenes de recopilación

Para crear conectores en agentes, puede emplear el asistente de configuración de orígenes de recopilación.

Para abrir el asistente de implementación de conector masivo

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la carpeta Explorador de agente y, a continuación, haga clic en Configurar orígenes de recopilación: 

Aparece el asistente de configuración de orígenes de recopilación.

Al emplear el asistente:

- Haga clic en Guardar para aplicar las actualizaciones sin cerrar el asistente. Aparecerá un mensaje de confirmación.
- Haga clic en Guardar y cerrar para aplicar las actualizaciones y cerrar el asistente. No aparece ningún mensaje de confirmación.

Selección de detalles del origen

Seleccione detalles del origen e identifique qué integración desea conectar a cada origen de evento. Debe disponer de una lista con los detalles de origen de evento necesarios en un archivo .csv para poder realizar este paso.

Nota: El archivo .csv contiene la información necesaria para crear los conectores. Cada columna del archivo .csv identifica un campo de configuración del conector y contiene valores para dicho campo. Por ejemplo, puede tener una columna de direcciones IP en la que figuren las direcciones IP de los host de los que desea recibir eventos.

La sección [Creación de una integración](#) (en la página 605) contiene campos de configuración específicos por tipo de sensor de registro

Para seleccionar detalles del origen

1. Abra el asistente de implementación del conector masivo.
2. Seleccione la integración que emplean sus orígenes en la lista desplegable Integración.
3. Seleccione la versión de integración en la lista desplegable Versión.
4. Vaya a la ubicación en la que ha guardado el archivo de origen de la recopilación que desea emplear. El origen de la recopilación debe ser un archivo .csv.

Las 100 primeras filas del archivo de origen de la recopilación seleccionado aparecen en el área de contenido del archivo de origen para realizar la revisión. La primera fila se define como la fila del encabezado de la columna y permanece como tal aunque ajuste el tamaño del ejemplo en el paso 5.

5. Utilice las listas desplegables Desde la fila y Hasta la fila para limitar la parte del archivo de origen de la recopilación que desea emplear.

La parte del archivo de origen de la recopilación seleccionado aparece en el área de contenido del archivo de origen para realizar la revisión. Los encabezados de las columnas no se ven afectados por los cambios realizados en Desde la fila con un valor superior a 1.

6. Vaya al paso siguiente.

Más información:

[Creación de una integración](#) (en la página 605)

Aplicación de reglas de supresión

Puede seleccionar las reglas de supresión que desea aplicar al cambio de configuración masivo.

Para aplicar reglas de supresión

1. Abra el asistente de implementación de conector masivo y vaya al paso de aplicación de reglas de supresión.
2. Seleccione cuáles de las reglas disponibles desea aplicar mediante el control de cambio.

Nota: Puede buscar reglas de supresión mediante el campo Patrón de reglas de supresión.

3. Vaya al paso siguiente.

Aplicación de reglas de resumen

Puede seleccionar las reglas de resumen que desea aplicar al cambio de configuración masivo.

Para aplicar reglas de resumen

1. Abra el asistente de implementación de conector masivo y vaya al paso de aplicación de reglas de resumen.
2. Seleccione cuáles de las reglas disponibles desea aplicar mediante el control de cambio.

Nota: Puede buscar reglas de resumen mediante el campo Patrón de las reglas de resumen.

3. Vaya al paso siguiente.

Configuración del conector

Puede establecer la configuración del conector para la creación de la conexión masiva. Cada conector que cree comparte las configuraciones establecidas en este paso, tanto mediante los orígenes recopilados del archivo .csv en el paso 1 como mediante las configuraciones guardadas.

Para establecer configuraciones de conectores

1. Abra el asistente de implementación de conector masivo y vaya al paso de configuración de conectores.

La página muestra los campos de origen definidos en el paso 1. Cada columna de encabezado del archivo de origen aparece como campo de origen. La página también muestra las configuraciones del sensor predeterminado para la integración seleccionada en el área de configuración de sensores.

2. Defina la configuración del conector mediante uno de estos dos procedimientos:
 - Seleccione una configuración guardada en la lista desplegable correspondiente.
 - Establezca las configuraciones individuales en el área de configuración de sensores arrastrando y soltando entradas del campo de origen en los campos de entrada de configuración deseados. Establezca de forma manual los campos necesarios para los que no hay valores de campo de origen.

Por ejemplo, la lista de origen contiene una columna Nombre de usuario. Arrástrela al campo de configuración de sensores de nombre de usuario si existe uno para el tipo de sensor que configura.
3. (Opcional) Haga clic en Repetir para agregar más campos de configuración de sensores según sea necesario.
4. Vaya al paso siguiente.

Selección de agentes y asignación de orígenes

Puede seleccionar los agentes en los que desea crear los conectores configurados. Asigne los orígenes de eventos seleccionados en el paso 1 a los agentes que desea establecer como destino para la implementación del conector.

Para seleccionar agentes y asignar orígenes

1. Abra el asistente de implementación de conector masivo y vaya al paso de selección de agentes y asignación de orígenes.

La página muestra una lista de orígenes basada en los orígenes cargados en el paso 1. Cada origen se numera en el orden de las filas, de manera que el Origen 1 representa la primera fila especificada en la lista de orígenes.
2. Busque los agentes que desee establecer como destinos por grupo de agentes, plataforma o nombre de agente.
3. Arrastre los orígenes deseados a cada carpeta de agentes de destino y haga clic para guardar la asignación de conectores.
4. Haga clic en Guardar o en Guardar y cerrar.

Los conectores basados en los orígenes que ha seleccionado se configuran en los agentes seleccionados.

Actualización de varias configuraciones de conectores

Puede actualizar varios conectores que utilicen el mismo sensor de registros cambiando uno o más configuraciones predeterminadas. Por ejemplo, podría cambiar el tipo de rotación de archivos de registro en varios conectores con el sensor de archivos de registro.

Para actualizar varias configuraciones de conectores

1. Haga clic en la ficha Administración y, a continuación, en la subficha Biblioteca.
2. Expanda las carpetas Biblioteca de refinamiento de eventos, Integraciones y Suscripción.
3. Seleccione una integración que utilice el sensor de registro del tipo al que desee aplicar las modificaciones de configuración.
4. Haga clic en Aplicar actualización por lotes a los conectores: 
Aparecerá el asistente de actualización de conectores y mostrará la página Selección de conectores.
5. Seleccione los conectores los que desee aplicar las actualizaciones y diríjase a la página Configuraciones predeterminadas.
6. Introduzca el valor que desee en los campos que desee actualizar y marque la casilla junto a ellos.
7. Haga clic en Ejecutar.
Aparecerá un mensaje de confirmación.

Capítulo 17: Correlación de eventos y gestión de incidentes

Esta sección contiene los siguientes temas:

[Tareas de regla de correlación](#) (en la página 641)

[Tareas de gestión de incidentes](#) (en la página 655)

[Consulta de detalles de incidentes](#) (en la página 656)

Capítulo 18: Tareas de regla de correlación

Las reglas de correlación pueden comunicar patrones de eventos, lo que le ayuda a identificar actividades sospechosas o condiciones peligrosas en su entorno. Cada vez que los eventos coincidan con los criterios de una regla de correlación, CA Enterprise Log Manager crea un incidente.

Puede realizar las siguientes tareas de regla de correlación si posee el rol de Administrador:

- Crear, editar o suprimir una regla de correlación.
- Crear un grupo de reglas de correlación.
- Importar o exportar una regla de correlación.
- Aplicar reglas de correlación y asociar destinos de notificación en su entorno.

Esta sección contiene los siguientes temas:

[Acerca de las reglas de correlación](#) (en la página 642)

[Uso de reglas de correlación predefinidas](#) (en la página 643)

[Uso de listas con claves con reglas de correlación](#) (en la página 647)

[Ejemplo: Creación de un archivo CSV para realizar pruebas](#) (en la página 648)

[Acerca de las notificaciones de incidentes](#) (en la página 648)

[Cómo diseñar y aplicar notificaciones de incidentes](#) (en la página 650)

Acerca de las reglas de correlación

Es posible aplicar reglas de correlación predefinidas, utilizar el asistente de reglas de correlación para crear reglas de correlación personalizadas para el entorno o modificar reglas existentes. Las reglas de correlación le permiten identificar grupos de eventos que pueden indicar ataques u otros riesgos de seguridad. Debe poseer el rol de Administrador para crear o editar reglas de correlación.

Cuando crea una regla de correlación, debe seleccionar cuál de los tres tipos desea crear. La plantilla de regla controla qué evento o eventos se consideran un incidente. Están disponibles las siguientes plantillas:

- Filtro sencillo: le permite buscar un solo evento o estado. Esta plantilla crea un incidente a partir de un solo evento.
- Plantilla de recuento: le permite buscar un conjunto de eventos idénticos. Se puede controlar el número de eventos del mismo tipo que debe buscar la regla. Cada vez que la regla detecta el número de eventos establecido, esta activa un incidente.
- Plantilla de transición de estado: le permite buscar una serie de eventos relacionados. Cuando se produce un evento o estado específico, seguido de otros eventos o estados, la regla crea un incidente. Puede definir los estados que la regla deba buscar y establecer el número de estados.

Nota: Para lograr una correlación efectiva, es necesario disponer de una vista completa de los eventos entrantes. Por esta razón se debería valorar la posibilidad de evitar aplicar reglas de supresión o de resumen al nivel del agente. Los eventos que se supriman o se resuman al nivel del agente no se tienen en cuenta para la correlación ni para la creación de incidentes.

La correlación de eventos puede dar lugar a tráfico de red significativo. Por esta razón, se puede valorar la posibilidad de asignar un servidor de correlación dedicado. Si desea obtener más información sobre los roles de servidor, puede consultar la *Guía de implementación de CA Enterprise Log Manager*.

En caso de que haya más mensajes de incidente de los que el servicio de correlación pueda procesar, éste servicio mantiene una cola de hasta 10.000 mensajes. El resto de mensajes se perderán. CA Enterprise Log Manager generará un evento autocontrolado si esto sucede.

Más información:

[Acerca de las notificaciones de incidentes](#) (en la página 648)

Uso de reglas de correlación predefinidas

CA Enterprise Log Manager proporciona un gran número de reglas de correlación predefinidas para utilizar en su entorno, organizadas por requisito de tipo o legal. Por ejemplo, en la carpeta de Reglas de correlación de la interfaz Biblioteca, se encuentra la carpeta PCI, que contiene reglas para diversos requisitos de PCI. También está la carpeta Identidad, que contiene reglas de uso general sobre autorización y autenticación.

Hay tres tipos principales de reglas, que se pueden incluir en cada categoría. Este tema muestra un ejemplo sobre cómo elegir y aplicar una regla de cada tipo.

Ejemplo: Selección y aplicación de una regla sencilla

Las reglas de correlación sencillas detectan la presencia de un estado o repetición. Por ejemplo, puede aplicar una regla que le alerte para la actividad de creación de cuentas fuera del horario de oficina normal. Antes de aplicar cualquier regla, debe asegurarse de que ha creado los destinos de notificación que desee para su entorno.

Para seleccionar y aplicar la regla Creación de cuentas fuera del horario de oficina

1. Haga clic en la ficha Administración, a continuación, en la subficha Biblioteca, y expanda la carpeta Reglas de correlación.
2. Expanda la carpeta PCI, después la carpeta Requisito 8 y seleccione la regla Creación de cuentas fuera del horario de oficina.

En el panel derecho aparecerán los detalles de la regla.

3. Revise los detalles de la regla para asegurarse de que la regla es apropiada para su entorno. En este caso, los filtros definen la acción de creación de cuentas, y establecen los horarios comerciales normales en hora y día de la semana.
4. (Opcional) Haga clic en Editar en la parte superior del panel para modificar la configuración del filtro, en caso de que sea necesario. Por ejemplo, podría cambiar el horario de trabajo normal para ajustarse a sus especificaciones locales.

Se abrirá el asistente de gestión de reglas con los detalles de la regla introducidos.

5. Agregue cualquier detalle de notificación que desee en el asistente de gestión de reglas. Los detalles de notificación proporcionan el contenido del mensaje que se proporciona en función de lo que se especifique en los destinos de notificación.

6. Una vez que haya terminado de preparar la regla, haga clic en Guardar y cerrar en el asistente. Cuando edita y guarda una regla de correlación predefinida, CA Enterprise Log Manager crea automáticamente una nueva versión y conserva la versión original.
7. Haga clic en la subficha Servicios y, a continuación, expanda el nodo Servicio de correlación.
8. Seleccione el servidor en el que desea aplicar la regla. Si ha identificado un servidor de correlación debe seleccionar dicho servidor.
9. Haga clic en Aplicar en el área Configuración de regla, y seleccione la nueva versión de la regla Creación de cuentas fuera del horario comercial normal, junto con el destino de notificación que desee que esté asociado a la regla.
10. Haga clic en Aceptar para cerrar el cuadro de diálogo y activar la regla.

Ejemplo: Selección y aplicación de una regla de recuento

Las reglas de correlación de recuento identifican una serie de estados o repeticiones idénticos. Por ejemplo, es posible aplicar una regla que le alerta sobre la ocurrencia de cinco o más inicios de sesión erróneos por una cuenta de administrador. Antes de aplicar cualquier regla, debe asegurarse de que ha creado los destinos de notificación que desee para su entorno.

Para seleccionar y aplicar la regla 5 inicios de sesión erróneos por cuenta de administrador.

1. Haga clic en la ficha Administración, a continuación, en la subficha Biblioteca, y expanda la carpeta Reglas de correlación.
2. Expanda la carpeta Gestión de las amenazas, a continuación la carpeta Actividad de inicio de sesión y cuenta sospechosas, y seleccione la regla "5 inicios de sesión erróneos por cuenta de administrador".

En el panel derecho aparecerán los detalles de la regla.

3. Revise los detalles de la regla para asegurarse de que la regla es apropiada para su entorno. En este caso, los filtros definen una cuenta de administrador como un nombre del usuario que pertenece a la lista con claves 'Administradores', y establecen el umbral de recuento a 5 eventos en 60 minutos.
4. (Opcional) Haga clic en Editar en la parte superior del panel para modificar la configuración del filtro, en caso de que sea necesario. Por ejemplo, podría cambiar el umbral de tiempo a 3 eventos en 30 minutos.

Se abrirá el asistente de gestión de reglas con los detalles de la regla introducidos.

5. Agregue cualquier detalle de notificación que desee en el asistente de gestión de reglas. Los detalles de notificación proporcionan el contenido del mensaje que se proporciona en función de lo que se especifique en los destinos de notificación.
6. Una vez que haya terminado de preparar la regla, haga clic en Guardar y cerrar en el asistente. Cuando edita y guarda una regla de correlación predefinida, CA Enterprise Log Manager crea automáticamente una nueva versión y conserva la versión original.
7. Haga clic en la subficha Servicios y, a continuación, expanda el nodo Servicio de correlación.
8. Seleccione el servidor en el que desea aplicar la regla. Si ha identificado un servidor de correlación debe seleccionar dicho servidor.
9. Haga clic en Aplicar en el área Configuración de regla, y seleccione la nueva versión de la regla 5 inicios de sesión erróneos por cuenta de administrador, junto con el destino de notificación que desee que esté asociado a la regla.
10. Haga clic en Aceptar para cerrar el cuadro de diálogo y activar la regla.

Ejemplo: Selección y aplicación de una regla de transición de estado

Las reglas de correlación de transición de estado identifican a su vez una serie de estados o repeticiones. Por ejemplo, se puede aplicar una regla que le alerte sobre la ocurrencia de inicios sesión erróneos seguidos de un inicio de sesión correcto de la misma cuenta de usuario. Antes de aplicar cualquier regla, debe asegurarse de que ha creado los destinos de notificación que desee para su entorno.

1. Haga clic en la ficha Administración, a continuación, en la subficha Biblioteca, y expanda la carpeta Reglas de correlación.
2. Expanda la carpeta Identidad, a continuación la carpeta Autenticación y seleccione la regla Inicios de sesión erróneos seguidos de un inicio de sesión correcto.

En el panel derecho aparecerán los detalles de la regla.

3. Revise los detalles de la regla para asegurarse de que la regla es apropiada para su entorno. En este caso, el panel de detalles muestra los dos estados que sigue la regla. El primero es cinco o más inicios de sesión erróneos por la misma cuenta de usuario o identidad. El segundo es un inicio de sesión correcto por ese mismo usuario o identidad.
4. (Opcional) Haga clic en Editar en la parte superior del panel para modificar la configuración de estado, en caso de que sea necesario.

Se abrirá el asistente de gestión de reglas y mostrará los dos estados que constituyen la regla.

5. Haga doble clic en cualquier estado que desee modificar.
Aparecerá el asistente de definición del estado y mostrará los detalles del estado.
6. Realice cualquier cambio de estado que desee al estado seleccionado y haga clic en Guardar y cerrar para volver al asistente de gestión de reglas. Por ejemplo, el primer estado busca 5 inicios de sesión erróneos en 10 minutos. Es posible cambiar el umbral de inicio de sesión erróneo, el tiempo, o ambos.
7. Agregue cualquier detalle de notificación que desee en el asistente de gestión de reglas. Los detalles de notificación proporcionan el contenido del mensaje que se proporciona en función de lo que se especifique en los destinos de notificación.
8. Una vez que haya terminado de preparar la regla, haga clic en Guardar y cerrar en el asistente. Cuando edita y guarda una regla de correlación predefinida, CA Enterprise Log Manager crea automáticamente una nueva versión y conserva la versión original.
9. Haga clic en la subficha Servicios y, a continuación, expanda el nodo Servicio de correlación.
10. Seleccione el servidor en el que desea aplicar la regla. Si ha identificado un servidor de correlación debe seleccionar dicho servidor.
11. Haga clic en Aplicar en el área Configuración de regla, y seleccione la nueva versión de la regla Inicios de sesión erróneos seguidos por una regla correcta, junto con el destino de notificación que desee que esté asociado a la regla.
12. Haga clic en Aceptar para cerrar el cuadro de diálogo y activar la regla.

Más información:

[Acerca de las notificaciones de incidentes](#) (en la página 648)

[Acerca de las reglas de correlación](#) (en la página 642)

[Establecimiento de valores predeterminados de notificación](#) (en la página 651)

Uso de listas con claves con reglas de correlación

Todas las reglas de correlación se crean a partir de uno o más filtros. Algunos filtros de reglas predefinidos están diseñados para seleccionar todos los valores de una tabla determinada en la que un campo de atributo contiene un valor utilizado como criterio para compilar la lista de valores de clave.

Es posible utilizar listas con claves en la creación, aplicación o correlación de reglas para proporcionar los valores predefinidos o personalizados a los filtros de regla. También se pueden actualizar las listas de valores con claves de forma manual o automática para asegurar que éstas permanecen actualizadas. Se pueden utilizar listas con claves con las reglas de correlación, tal y como se hace con los informes.

Si desea obtener más información sobre cómo emplear listas con claves, puede consultar el capítulo Consultas e informes de esta guía.

Más información:

[Preparación para el empleo de informes mediante listas con clave](#) (en la página 350)

[Enfoques para el mantenimiento de listas con clave](#) (en la página 355)

[Creación de valores con clave para informes predefinidos](#) (en la página 365)

Ejemplo: Creación de un archivo CSV para realizar pruebas

Este ejemplo ilustra la creación de un archivo CSV para pruebas de reglas de correlación. Está pensado para probar una regla que busca 5 inicios de sesión erróneos seguidos de un inicio de sesión correcto de un único usuario.

Para crear un archivo CSV para probar un inicio de sesión erróneo seguido por una regla correcta

1. Inicie sesión en CA Enterprise Log Manager como Administrador, y haga clic en la ficha Consultas y la ficha Informes.
2. Busque la consulta "Cinco inicios de sesión erróneos en la última hora por ejecutor".
3. Ejecútela y consulte los resultados. Si hay resultados, continúe al paso siguiente. Si no hay resultados, cree un usuario ficticio, cierre sesión y produzca inicios de sesión erróneos con el nuevo usuario ficticio.
4. Exporte la consulta a CSV y abra el archivo CSV en Excel.
5. Agregue otros detalles del usuario según sea necesario. Por ejemplo, puede agregar información para reflejar el inicio de sesión correcto.
6. Guarde el archivo CSV cuando posea toda la información del evento que necesite.
7. Abra la regla que se desee probar en el explorador de la biblioteca, y haga clic en la ficha Prueba de regla en el panel de detalles.
8. Cargue el archivo CSV, y confirme que se han creado los incidentes correctos.

Acerca de las notificaciones de incidentes

Es posible establecer notificaciones, que pasen información acerca de un incidente, para que se activen automáticamente al crear un incidente; o iniciarlas manualmente después de haber consultado el incidente. En cualquiera de los dos casos, debe definir primero los destinos de notificación que desee utilizar en su entorno.

Deben crear notificaciones en dos partes:

1. Destino de notificación, que puede contener cualquier combinación de los tipos de destino disponibles. Por ejemplo, un destino podría contener direcciones de correo electrónico, credenciales de servidores SNMP, y un nombre del proceso de CA IT PAM. Se pueden asignar destinos a varias reglas.
2. Detalles de notificación, que se agregan a reglas individuales, y contienen la información proporcionada por la notificación; asuntos y texto de correos electrónicos, datos de SNMP, parámetros del proceso de CA IT PAM, por ejemplo.

Las notificaciones automáticas requieren una regla de correlación con detalles de notificación y un destino de notificación asociado. Si los dos componentes están presentes, cada vez que la regla cree un incidente, se enviará una notificación automática al destino o destinos especificados. La combinación de destinos y detalles le permite establecer notificaciones modulares. Por ejemplo, podría enrutar la misma información de notificación a diferentes centros de servicio al usuarios regionales o personal de TI.

Puede asignar también destinos de incidentes existentes. Cuando abre un incidente y asigna un destino de notificación, los detalles de notificación especificados en la regla se envían inmediatamente. La regla debe incluir notificaciones para enviar notificaciones manuales.

Más información:

[Establecimiento de valores predeterminados de notificación](#) (en la página 651)

[Acerca de las reglas de correlación](#) (en la página 642)

Cómo diseñar y aplicar notificaciones de incidentes

Se pueden establecer notificaciones para sus reglas de correlación. Las notificaciones le permiten pasar información clave sobre incidentes detectados al personal que especifique, o crear de forma automática tickets de centro de servicio al usuario de CA IT PAM.

Utilice el siguiente proceso para diseñar y establecer notificaciones en su entorno:

1. Planee y cree destinos de notificación.
2. Seleccione las reglas de correlación predefinidas, o cree las reglas personalizadas que desee utilizar en su entorno.
3. Agregue detalles de notificación a las reglas para las que desee establecer notificaciones.
4. Aplique las reglas de correlación a los servidores de CA Enterprise Log Manager, y asigne los destinos de notificación.

Más información:

[Acerca de las reglas de correlación](#) (en la página 642)

[Establecimiento de valores predeterminados de notificación](#) (en la página 651)

[Consideraciones del servicio de correlación](#) (en la página 167)

Establecimiento de valores predeterminados de notificación

Es posible establecer detalles de notificación en una regla, lo que especifica el contenido de la notificación pero no los destinos. Por ejemplo, puede establecer la línea de asunto y texto de contenido de un correo electrónico, pero no las direcciones de envío, que están controladas por los destinos de notificación. Este sistema le permite configurar contenido estándar (utilizando detalles), que se puede enviar a diversos destinatarios (utilizando destinos).

Se puede incluir cualquier combinación de los tipos de notificación disponibles en los detalles de notificación de una sola regla.

Para establecer los detalles de notificación

1. Abra al asistente de reglas de correlación, introduzca las definiciones de regla necesarias, y avance hasta llegar al paso Detalles de notificación.
2. Seleccione la ficha del correo electrónico y siga los siguientes pasos para agregar información de notificación de correo electrónico:
 - a. Introduzca una línea de asunto para el correo electrónico de la notificación.
 - b. (Opcional) Si introduce texto en cualquiera de los campos de la ficha del correo electrónico, puede utilizar la lista desplegable Campos de datos y el botón Agregar para insertar variables de campo de datos. Por ejemplo, podría elegir agent_address y hacer clic en Agregar.

"%agent_address%" aparece en el campo de texto. Cuando una regla genera un correo electrónico, aparece el valor del campo agent_address en lugar de la variable.
 - c. Introduzca el cuerpo del mensaje para el correo electrónico de notificación.

Nota: El cuerpo del mensaje se crea en formato HTML, por lo que todo el texto aparece en una línea. Para crear un salto de línea, introduzca
 al final de la línea de texto.
3. Seleccione la ficha Proceso y siga los siguientes pasos para agregar parámetros del proceso de CA IT PAM:
 - a. Introduzca el nombre de un proceso de CA IT PAM al que desee pasar la información del incidente, como:
/CA_ELM/EventAlertOutput
 - b. Haga clic en Agregar parámetro para especificar un parámetro y su valor.

Aparecerá el cuadro de diálogo Agregar parámetro de proceso.

- c. Escriba un nombre de parámetro en el campo Nombre, por ejemplo 'Severidad'.
- d. Defina un valor escribiéndolo en el área de valor, o seleccionando un campo de gramática de eventos comunes en la lista desplegable y haciendo clic en Agregar campo de datos. La información del evento del campo de gramática de eventos comunes que especifique se pasa a dicho parámetro. Continuando con el ejemplo del paso anterior, podría seleccionar 'event_severity' para presentar el valor del campo event_severity como el parámetro de severidad de CA IT PAM.
- e. Repita los pasos a-c para agregar parámetros y valores adicionales, según sea necesario.
- f. Cuando haya agregado todos los campos de gramática de eventos comunes que desee para el parámetro actual, haga clic en Aceptar.

Nota: Es posible escribir y agregar varios campos de gramática de eventos comunes según sea necesario para definir un parámetro. Por ejemplo, si desea definir el parámetro de descripción para una notificación utilizado con una regla de averiguación de contraseñas, podría introducir:

Este incidente informa de que se han producido cuatro inicios de sesión erróneos por %dest_identity_unique_name% en %dest_hostname% en 10 minutos.

La estructura de %value% es el resultado de seleccionar un campo de gramática de eventos comunes y utilizar el botón Agregar campo de datos tal y como se describe en el paso b.

- 4. Seleccione la ficha SNMP y siga los siguientes pasos para agregar la configuración de mensajes SNMP:
 - a. Ajuste el ID del mensaje SNMP personalizado según lo requiera su destino de transmisión de SNMP.
 - b. Introduzca en el área de entrada el nombre del campo de gramática de eventos comunes que desee enviar. A medida que escribe en el campo, se delimitan las opciones disponibles en la lista desplegable.
 - c. Haga clic en Agregar.
 - d. El nombre del campo de gramática de elementos comunes aparece en el área de campos seleccionada. Cualquier información del evento en ese campo se envía para reglas que utilicen esta plantilla de notificación. Debe seleccionar al menos un campo de gramática de eventos comunes.
 - e. Repita los pasos b-c para enviar campos de gramática de eventos comunes adicionales.

5. Haga clic en la flecha apropiada para avanzar al paso del asistente que desee completar a continuación o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, la nueva regla aparecerá en la carpeta adecuada; de no ser así, aparecerá el paso seleccionado.

Más información:

[Acerca de las reglas de correlación](#) (en la página 642)

[Acerca de las notificaciones de incidentes](#) (en la página 648)

Capítulo 19: Tareas de gestión de incidentes

Un incidente de CA Enterprise Log Manager se compone de uno o más eventos, identificados y vinculados por una regla de correlación. Cada vez que una regla de correlación detecta un evento o varios eventos que cumplen sus criterios, CA Enterprise Log Manager crea un incidente.

Puede realizar las siguientes tareas de gestión de incidentes si posee el rol de Administrador:

- Consultar los detalles de incidentes creados por las reglas de correlación en su entorno.
- Filtrar la lista de incidentes, o establecer las condiciones de resultado para localizar incidentes particulares o tipos de incidentes, o delimitar su vista de incidente.
- Aplicar destinos de la notificación a incidentes existentes, controlando respuestas como la notificación de correo electrónico.
- Exportar información de incidentes.
- Programar alertas de acción basadas en un incidente.
- Combinar incidentes existentes en un nuevo incidente.

Nota: Puede obtener información detallada sobre las tareas de gestión de incidentes en la *ayuda en línea de CA Enterprise Log Manager*.

Consulta de detalles de incidentes

Puede consultar detalles de incidentes en su entorno, incluida la información de estado, prioridad e historial. Es posible consultar solamente los incidentes que se enrutan al servidor de correlación en el que inicia sesión. Puede controlar la forma en la que los servidores de CA Enterprise Log Manager enrutan los eventos, con sólo configurar el servicio de correlación.

Para consultar los detalles de incidentes

1. Haga clic en la ficha Incidentes, seleccione el incidente que se desee investigar, y haga doble clic en la fila de incidente.

Aparecerá el cuadro de diálogo Detalles, que muestra los detalles básicos del incidente, incluidos el nombre, la fecha y la severidad.

2. Cambie la configuración de Prioridad o Estado mediante los menús desplegables apropiados.
3. (Opcional) Haga clic en la ficha Historial para consultar información como la cantidad y la hora establecida de los eventos agregados al incidente, o de las notificaciones automáticas que se han iniciado.
4. Haga clic en Aceptar o Aplicar.

Más información:

[Consideraciones del servicio de correlación](#) (en la página 167)

Capítulo 20: Agentes

Esta sección contiene los siguientes temas:

[Planificación de la instalación de agentes](#) (en la página 657)
[Planificación de configuraciones de agentes](#) (en la página 661)
[Tareas de gestión de agentes](#) (en la página 666)
[Actualización de la clave de autenticación del agente](#) (en la página 667)
[Descarga de binarios del agente](#) (en la página 668)
[Configuración de un agente](#) (en la página 669)
[Visualización del cuadro de mandos de los agentes](#) (en la página 673)
[Visualización y control del estado de agentes o conectores](#) (en la página 675)
[Creación de grupos de agentes](#) (en la página 677)
[Configuración de la gestión de agentes](#) (en la página 680)
[Protección de los agentes contra el impacto de los cambios de dirección IP del servidor](#) (en la página 684)
[Aplicación de actualizaciones de suscripción](#) (en la página 687)
[Creación de un archivo de diagnóstico del agente para el Departamento de Soporte Técnico.](#) (en la página 691)

Planificación de la instalación de agentes

Al planificar la instalación de agentes, el planificador debe determinar cuántos agentes son necesarios y cuándo se deben instalar. Esta planificación puede llevarla a cabo quien instala los agentes, un administrador de redes o un arquitecto de sistemas.

Para planificar instalaciones de agentes

1. Cree una versión electrónica de la tabla de planificación de instalación de agentes que sea adecuada para registrar la información necesaria. Considere la posibilidad de usar la tabla de muestra y los encabezados de columna que aparecen a continuación.

Plataforma de origen de evento	Nombre de host o dirección IP donde se ejecuta el origen de evento	Uno de los siguientes: - Sin agente-Directo - Sin agente-Punto de recopilación - Agente en punto final	Nombre de host o dirección IP donde debe instalarse el agente

Plataforma de origen de evento	Nombre de host o dirección IP donde se ejecuta el origen de evento	Uno de los siguientes: - Sin agente-Directo - Sin agente-Punto de recopilación - Agente en punto final	Nombre de host o dirección IP donde debe instalarse el agente

2. Identifique cada origen de evento para que se centre en la recopilación de registros y guarde la ubicación y la plataforma en la tabla de planificación de agentes.

3. Tenga en cuenta los siguientes costes y ventajas de cada tipo de solución.

	Ventaja	Coste o limitación
Sin agente - Directo desde CA Enterprise Log Manager - Sin agente instalado	No es necesario instalar ningún agente.	Puede incluir únicamente la recopilación de aquellos orígenes de evento que sean compatibles con la plataforma del dispositivo de software. También se aplican los costes de la opción Sin agente-Punto de recopilación.
Sin agente - Agente en punto de recopilación	No es necesario instalar ningún agente en el host en el que se ejecuta el origen de evento. La consolidación de la recopilación en un punto común reduce el número de agentes que se deben instalar en comparación con la recopilación mediante agente.	Las reglas de supresión sólo se pueden aplicar en el servidor de CA Enterprise Log Manager. Esto carece de la ventaja que supone la reducción del tráfico en la red. La comunicación de eventos entre el origen y el servidor de CA Enterprise Log Manager no está cifrada. Debe ser posible acceder de forma remota al origen del evento.
Mediante agente - Agente en punto final	Puede aplicar reglas de supresión al origen en lugar de al servidor de CA Enterprise Log Manager. Esto reduce el tráfico de la red entre el punto de recopilación y el servidor de CA Enterprise Log Manager. La comunicación de registros entre el origen y el servidor de CA Enterprise Log Manager está cifrada. Puede incluir el volumen de eventos más elevado de las tres soluciones.	Debe instalarse un agente en el lugar en el que se ejecuta un origen de evento.

4. Registre la solución que desee para cada origen de evento.
5. Ordene la tabla de planificación de agentes por la columna 3 y, a continuación, por la columna 2. De este modo, se muestran todos los orígenes de eventos mediante agente que se ejecutan en el mismo host en bloques.

6. En el caso de orígenes de eventos asignados mediante agente, busque la primera aparición en un bloque con el mismo nombre y copie los datos de la columna 2 a la columna 4. El resultado es una sola entrada para cada host en el que se ejecutan uno o varios orígenes de eventos. (Nunca necesitará más de un agente en un host determinado, independientemente del número de orígenes de eventos.)
7. En el caso de orígenes de eventos asignados a Sin agente-Punto de recopilación, planifique dónde desea instalar los agentes del modo siguiente:
 - a. Identifique el número de puntos de recopilación necesarios para incluir los orígenes de eventos identificados como candidatos para agentes remotos.
 - b. Planifique las agrupaciones de orígenes de eventos identificados como candidatos para agentes remotos según el área de ubicación de red común.
 - c. Para cada grupo de orígenes de eventos, identifique el servidor que desea emplear como punto de recopilación. Puede tratarse de un servidor dedicado. Registre la decisión en la columna 4.
8. Si ha registrado orígenes de eventos para los que no hay una solución asignada y utiliza un adaptador de CA heredado, consulte la *Guía de implementación de CA Enterprise Log Manager* para obtener más detalles.
9. Entregue los datos registrados en la cuarta columna de la tabla de planificación de agentes al usuario que va a instalar los agentes.

Planificación de configuraciones de agentes

El usuario de EiamAdmin instala agentes en función de la determinación del método de recopilación óptimo. Entre los métodos evaluados se incluyen los siguientes:

- Recopilación de registros sin agente directamente desde el servidor de CA Enterprise Log Manager; a veces se denomina recopilación directa.
- Recopilación de registros sin agente desde un punto de recopilación.
- Recopilación basada en agente desde el host en el que se está ejecutando el origen del evento.

El análisis que precede a la instalación puede revelar parte de la información que necesita el administrador que configura los agentes y los conectores.

El primer paso para la configuración de agentes es obtener la hoja de datos de planificación de agentes del usuario EiamAdmin o la alternativa empleada para documentar la ubicación de instalación de los agentes. Después de configurar el primer administrador, el usuario de EiamAdmin entrega al administrador la hoja de trabajo de planificación de la instalación de agentes anotada. El primer administrador, a su vez, planifica los conectores necesarios para cada agente antes de comenzar la configuración.

El administrador configura cada agente instalado por el usuario EiamAdmin. Además, el administrador configura un conector para cada origen de evento, independientemente del método de recopilación (sin agente-directo, sin agente-punto de recopilación o mediante agente). El administrador configura los conectores en cada agente mientras está conectado al servidor de CA Enterprise Log Manager que va a recibir eventos recopilados por ese agente.

Nota: Cuantos menos conectores haya configurados en un agente, mejor será el rendimiento.

Una excepción de este proceso es cuando la instalación del agente se lleva a cabo en modo silencioso. En ese caso, es el instalador quien configura los conectores. Los conectores configurados en un agente permiten que el agente recopile eventos sin formato desde orígenes de eventos específicos. Los conectores convierten los eventos sin formato en eventos refinados y transmiten los eventos refinados a CA Enterprise Log Manager.

La creación de grupos de agentes es opcional. Si no se crean grupos de agentes personalizados, los agentes se asignan al grupo de agentes predeterminado. Los administradores crean grupos de agentes por los motivos siguientes:

- Para activar la creación de informes de eventos recopilados por agentes del mismo grupo de agentes.
- Para activar la asignación de un usuario administrativo diferente a distintos grupos de agentes. (El acceso de usuarios puede limitarse a grupos de agentes determinados con políticas de acceso.)

Los registros de eventos recopilados se envían a un servidor de CA Enterprise Log Manager para su procesamiento y almacenamiento inicial. Los administradores deben configurar el servidor que va a recibir los registros para cada agente o grupo de agentes. La asignación de un servidor a un grupo de agentes es un método rápido para asignar el servidor a todos los agentes del grupo de agentes.

Planificación de recopilación directa de registros

CA Enterprise Log Manager se instala con un agente predeterminado que se puede emplear para la recopilación directa de registros. Se denomina recopilación directa porque el empleo del agente predeterminado no requiere la instalación de ningún agente. El agente predeterminado puede recopilar eventos de casi cualquier origen de eventos, con las limitaciones siguientes.

- El sensor de registro debe poderse ejecutar en el dispositivo de software; algunos sensores de registro, como el sensor de registro WMI, están vinculados a una plataforma determinada.
- Debe ser posible acceder de forma remota al origen del evento.

Configure el agente predeterminado como configuraría un agente instalado de forma independiente. La recopilación directa de registros por parte del agente predeterminado es ideal para un sistema muy pequeño.

Orígenes de eventos para la recopilación de registros directa

CA Enterprise Log Manager ofrece sensores de registro que se pueden ejecutar en el servidor de CA Enterprise Log Manager para facilitar la recopilación de registros directa sin agente. En el momento de publicar este documento, la compatibilidad es la siguiente:

- syslog
- WinRM
- ODBC
- TIBCO

Para determinar las integraciones compatibles con el agente predeterminado

1. Seleccione un servidor de CA Enterprise Log Manager en el explorador de agente de la ficha Administración, en la subficha Recopilación de registros.
2. Haga clic en Crear nuevo conector.

La lista desplegable Integración incluye las integraciones con las que puede crear un conector para la implementación en el agente predeterminado. Cada integración, en la que se basan los conectores, se diseña para recuperar eventos de un origen de eventos determinado.

Para obtener una lista completa de sensores de registro e integraciones compatibles, consulte la página del producto de CA Enterprise Log Manager en el [servicio de Atención al cliente](#).

Nota: Un sensor de registro es un componente de integración diseñado para leer un tipo de registro específico, como una base de datos, syslog, un archivo o SNMP.

Planificación de recopilación de registros sin agente

La recopilación de registros sin agente se puede llevar a cabo mediante la instalación de un agente en un servidor de recopilación que recopila eventos de múltiples orígenes de eventos remotos.

Al planificar la configuración de la recopilación de registros sin agente desde un servidor de recopilación, tenga en cuenta lo siguiente:

- Cuantos menos conectores haya implementados en un agente, mejor será el rendimiento.
- El número máximo de conectores que debe configurar en un agente determinado depende de si el agente está instalado en un servidor dedicado, en la potencia de dicho servidor y en los tipos de orígenes de eventos que tenga como objetivo. Como regla general, no debería configurar más de 40 o 50 conectores en un solo agente.
- No se obtiene ninguna ventaja de rendimiento al agrupar en un mismo servidor de recopilación conectores del mismo tipo configurados en agentes distintos. Por extensión, no se obtienen ventajas en el rendimiento al direccionar eventos con los mismos tipos de orígenes de eventos a un servidor de CA Enterprise Log Manager determinado en una federación.

Planificación de recopilaciones de registros mediante agente

Después de que el instalador instale un agente en un servidor sin orígenes de eventos locales, los administradores configuran un conector en dicho agente para cada origen de eventos ejecutado en modo local.

Si hay varios servidores de destino con los mismos tipos de orígenes de eventos, puede agrupar dichos servidores de destino en un grupo de agentes y llevar a cabo la configuración del grupo de agentes.

La entrega garantizada puede ser un problema para la recopilación directa de syslogs. Para contrarrestarlo, configure una escucha de syslog en un agente instalado con el origen de eventos de syslog.

Selección del nivel que se va a configurar

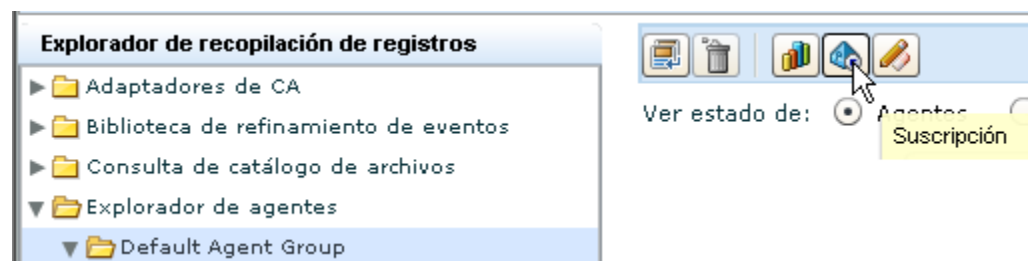
Las opciones Suscripción, Aplicación de reglas de supresión y Estado y comando pueden seleccionarse desde varios niveles. Por ejemplo, la configuración de Suscripción se puede iniciar desde los niveles siguientes:

- Explorador de agentes
- Grupo de agentes predeterminado o grupo de agentes definido por el usuario
- Agente

Para configurar una opción con la intención de que se aplique a todos los agentes de todos los grupos, seleccione Explorador de agentes y, a continuación, haga clic en el botón correspondiente a la acción que desea llevar a cabo.



Para configurar una opción de manera que se aplique a todos los agentes de un grupo seleccionado, seleccione el nombre del grupo y, a continuación, haga clic en el botón correspondiente a la acción que desea llevar a cabo.



Para configurar una opción de manera que sólo se aplique a un agente, seleccione el agente y, a continuación, haga clic en el botón correspondiente a la acción que desea llevar a cabo.



Tareas de gestión de agentes

El explorador de agentes le permite visualizar y gestionar los agentes de recopilación de eventos del entorno. Puede emplear la interfaz del explorador de agentes para llevar a cabo tareas de gestión en las áreas siguientes:

- Configuración de agentes: puede cambiar el nombre de los agentes, así como configurar los grupos a los que pertenecen y los grupos que tienen asociados.
- Grupos de agentes: puede agrupar agentes por ubicación geográfica, importancia empresarial o tipo de origen de evento, por ejemplo. También puede asignar agentes agrupados a diferentes servidores de CA Enterprise Log Manager según sea necesario.
- Suscripciones: puede visualizar y aplicar actualizaciones disponibles a agentes.
- Comando y estado de agentes: puede visualizar el estado actual de los agentes, así como detenerlos o activarlos según sea necesario.

Más información

[Descarga de binarios del agente](#) (en la página 668)

[Actualización de la clave de autenticación del agente](#) (en la página 667)

[Creación de grupos de agentes](#) (en la página 677)

[Aplicación de actualizaciones de suscripción](#) (en la página 687)

[Configuración de la gestión de agentes](#) (en la página 680)

Actualización de la clave de autenticación del agente

Puede ver y actualizar la clave empleada por los agentes para registrarse en el servidor de CA Enterprise Log Manager. La modificación periódica de esta clave permite evitar que se instalen agentes sin autorización en el entorno. De forma predeterminada, la clave es la misma para todos los servidores de CA Enterprise Log Manager en las instancias de aplicación. Sin embargo, puede definir esta clave para que sea exclusiva en cada instancia de aplicación.

El instalador de agentes debe introducir esta clave de agentes como código de autorización en el asistente de instalación del Agente.

Para actualizar la clave de autenticación del agente

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la carpeta Explorador de agentes.

Los botones de gestión de agentes aparecen en el panel de detalles.

3. Haga clic en Clave de autenticación del agente: 

Aparece el panel Clave de autenticación del agente.

4. Introduzca una clave nueva en los campos de introducción de clave y confirmación de clave y, a continuación, haga clic en Guardar.

Aparece un mensaje de confirmación de acción correcta.

Descarga de binarios del agente

Puede descargar binarios de agente e instalarlos en el equipo local sin emplear ningún otro medio de instalación.

Si desea obtener más información sobre la instalación de agentes, consulte la *Guía de instalación del Agente de CA Enterprise Log Manager*.

Para descargar archivos binarios de agente

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la carpeta Explorador de agentes.

Los botones de la gestión de agentes aparecerá en el panel de detalles.

3. Haga clic en Descargar archivos binarios de agente: 

Aparece la lista de archivos binarios de agente, que muestra los agentes disponibles y sus versiones actuales.

4. Haga clic en el agente que desee descargar.

Aparece el cuadro de diálogo de descarga.

5. Seleccione la ubicación en la que desea guardar el archivo binario del agente y haga clic en Guardar.

El archivo se guarda en la ubicación seleccionada y aparece un mensaje de confirmación.

Configuración de un agente

Puede configurar un agente instalado y registrado tras acceder a él en el explorador de agentes.

Para configurar agentes

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la lista de la carpeta Recopilación de registros.
2. Haga clic en la carpeta Explorador de agentes.
La carpeta se expande y muestra la carpeta de Grupo de agentes.
3. Seleccione el agente que desea configurar y haga clic en Editar en la parte superior del panel.
Aparecen los detalles del agente en el panel de detalles.
4. Realice los cambios deseados, incluidos los siguientes:

Nombre de usuario

Define el nombre de usuario con el que se ejecuta el agente.

Puerto

Establece el puerto que emplea el agente para comunicarse con CA Enterprise Log Manager.

Grupo de agentes

Define el grupo al que pertenece el agente.

Número máx. de archivos

Establece el número máximo de archivos que se pueden crear en la cola de archivos de recepción de eventos. El número máximo de archivos es 1.000.

Tamaño máx. por archivo

Establece el tamaño máximo, en MB, para cada archivo de la cola de archivos de recepción de eventos. Cuando un archivo alcanza el tamaño máximo, CA Enterprise Log Manager crea un archivo nuevo. El tamaño máximo es 2.048 MB.

Modo de envío de eventos

Define cuál de los siguientes estilos de transmisión es el que utiliza el agente:

- Conmutación por error: el agente envía eventos al primer servidor de la lista Servidores del gestor de registros. Si se interrumpe la comunicación, intentará establecer la comunicación con cada servidor en el orden establecido, hasta que se restaure la comunicación.
- Turno rotativo: el agente envía eventos a cada servidor de la lista Servidores del gestor de registros de forma sucesiva, para intentar ponerse en contacto con el siguiente servidor de la lista al cabo de una hora. Este período no se puede configurar.

Activar cifrado de eventos

Establece el agente que utilizará AES128 para cifrar los eventos que transmite. La activación del cifrado de eventos repercutirá en el rendimiento.

Activar programación de envío

Configura el agente para que únicamente envíe eventos durante un intervalo de tiempo determinado. Al activar la casilla de verificación Activar programación de envío, aparecen los campos Fecha y hora de inicio y Fecha y hora de finalización. Escriba los valores de hora GMT que desee expresada con el formato de 24 horas, conforme a los siguientes requisitos:

- Debe haber, como mínimo, una hora de diferencia entre los valores de fecha y hora de inicio y de finalización.
- Si el valor de la fecha y hora de inicio es superior al valor de la fecha y hora de finalización, ésta se establece en el día siguiente a la fecha y hora de inicio. Por ejemplo, si establece la hora de inicio a las 23 y la hora de finalización a las 6, el intervalo de tiempo de la transmisión abarca desde las 11 p. m. GMT hasta las 6 a. m. GMT del día siguiente.

Reemplazar la dirección IP por el nombre de host

Establece el agente para reemplazar la dirección IP de un origen del evento por el nombre de host del origen del evento. Todos los conectores del agente heredan esta función. Si desea activar la función para todos los agentes de su entorno, configure cada agente por separado. Si activa esta función, CA Enterprise Log Manager reemplaza la dirección IP por el nombre de host para los campos de la gramática de eventos comunes siguientes:

- source_hostname
- dest_hostname
- agent_hostname
- event_source_hostname
- receiver_hostname

Servidores del gestor de registros

Controla los servidores de CA Enterprise Log Manager a los que el agente enruta eventos, así como el orden en el que se debe conectar con ellos. Puede emplear el control de cambio para seleccionar los servidores disponibles y los botones de flecha situados a la derecha de los servidores seleccionados para establecer la prioridad de comunicación.

Nota: Actualice los servidores de CA Enterprise Log Manager antes de actualizar los agentes. Los servidores de CA Enterprise Log Manager admiten agentes con el mismo número de versión o un número inferior al actual. Para ayudar a garantizar un almacenamiento adecuado de los eventos recopilados al configurar o actualizar agentes, compruebe que el agente sólo envía eventos a servidores de CA Enterprise Log Manager cuyo nivel es igual o superior al del agente.

5. Haga clic en Guardar.

Más información

[Creación de grupos de agentes](#) (en la página 677)

Control de archivos de configuración manipulada

Los agentes utilizan un archivo de configuración que se encuentra almacenado en la memoria mientras se encuentran en ejecución. Si alguien manipula un archivo de configuración mientras el agente se está ejecutando, el agente no utiliza el archivo manipulado. Cuando un agente recibe una configuración nueva desde el servidor de CA Enterprise Log Manager, el agente sustituye el archivo del disco por el archivo recibido antes de reiniciarse. De este modo, se sustituyen los archivos manipulados por el archivo correcto.

Si alguien reinicia el agente desde un origen externo después de manipular el archivo, el agente detecta que el archivo está manipulado y se cierra. El agente no acepta ningún dato de configuración, incluida la lista del servidor de CA Enterprise Log Manager del archivo manipulado.

El Explorador de agente indica que el agente no responde. Utilice el estado del servidor de CA Enterprise Log Manager y las herramientas de comando para restablecer la configuración del agente. El agente sigue trabajando correctamente tras realizar esta acción.

Visualización del cuadro de mandos de los agentes

El usuario puede consultar el cuadro de mandos de agente para visualizar el estado de los agentes en el entorno. El cuadro de mandos también muestra detalles como el modo de FIPS actual (FIPS o no-FIPS), y los detalles de uso. Éstos incluyen eventos por segunda carga, uso del porcentaje de CPU, y la fecha y hora de actualización más recientes.

Para visualizar el cuadro de mandos de agentes

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Seleccione la carpeta Explorador de agente.

Los botones de la gestión de agentes aparecerá en el panel de detalles.

3. Haga clic en Cuadro de mandos y controlador de estado de los agentes: 

Aparece el panel de búsqueda de agentes, que muestra el estado de todos los agentes disponibles en un gráfico detallado. Por ejemplo:

Total: 10; En ejecución: 8; Pendiente: 1; Detenido: 1; No responde: 0

4. (Opcional) Seleccione criterios de búsqueda de agentes para restringir la lista de agentes mostrados. Puede seleccionar uno o más de los criterios siguientes:
- Grupo de agentes: sólo devuelve los agentes asignados al grupo seleccionado
 - Plataforma: sólo devuelve los agentes que se ejecutan en la plataforma seleccionada
 - Estado: sólo devuelve los agentes que tengan el estado seleccionado como, por ejemplo, En ejecución.
 - Patrón de nombres de agentes: sólo devuelve los agentes que contienen el patrón especificado
5. Haga clic en Mostrar estado.

Aparece una lista de agentes que cumplen los criterios de búsqueda, en la que aparece, entre otra, la información siguiente:

- Nombre y versión del conector local
- Servidor de CA Enterprise Log Manager actual
- Modo de FIPS de agente (FIPS o no-FIPS)
- Último dato de carga de eventos registrados por segundo realizada por el agente
- Último valor registrado de uso de la CPU
- Último valor registrado de uso de la memoria
- Actualización de configuración más reciente
- Estado de la actualización de configuración

Visualización y control del estado de agentes o conectores

Puede controlar el estado de los agentes o conectores de su entorno, reiniciar agentes así como iniciar, detener y reiniciar conectores cuando sea necesario.

Puede ver agentes o conectores desde distintos niveles de la jerarquía de carpetas del explorador de agente. Cada nivel reducirá la vista disponible de forma correspondiente:

- Desde la carpeta del explorador de agente, podrá ver todos los agentes o conectores asignados al servidor de CA Enterprise Log Manager actual.
- Desde la carpeta de un grupo de agentes específico, podrá ver los agentes y los conectores asignados a ese grupo de agentes.
- Desde un agente individual, sólo podrá ver ese agente y los conectores asignados a éste.

Puede determinar el modo de FIPS (FIPS o no FIPS) para un agente desde los tres niveles.

Para ver el estado del agente o del conector

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Seleccione la carpeta Explorador de agente.

Los botones de la gestión de agentes aparecerá en el panel de detalles.

3. Haga clic en Estado y comando: 

Aparecerá el panel de estado.

4. Seleccione Agentes o Conectores.

Aparecerá el panel de búsqueda de agentes o conectores.

5. (Opcional) Seleccione los criterios de búsqueda de actualización de agentes o conectores. Si no introduce ningún término de búsqueda, aparecerán todas las actualizaciones disponibles. Se pueden seleccionar uno o más de los siguientes criterios para limitar la búsqueda:

- Grupo de agentes: sólo devuelve los agentes y los conectores asignados al grupo seleccionado.
- Plataforma: sólo devuelve los agentes y conectores que se ejecutan en el sistema operativo seleccionado.
- Patrón de nombres de agentes: sólo devuelve los agentes y conectores que contienen el patrón especificado.
- (Sólo conectores) Integración: sólo devuelve los conectores que utilizan la integración seleccionada.

6. Haga clic en Mostrar estado.

Aparece un gráfico de detalles que muestra el estado de los agentes o conectores que se ajustan a la búsqueda. Por ejemplo:

Total: 10; En ejecución: 8; Pendiente: 1; Detenido: 1; No responde: 0

Nota: Si actualiza la configuración de un agente, CA Enterprise Log Manager necesitará un máximo de cinco minutos para sincronizar el estado actualizado de este agente con los otros agentes dentro de una federación.

7. (Opcional) Haga clic en la pantalla de estado para ver los detalles del panel Estado en la parte inferior del gráfico.

Nota: Puede hacer clic en el botón A petición para que un agente o conector actualice la pantalla de estado.

8. (Opcional) Si ve conectores, seleccione cualquier conector y haga clic en Reiniciar, Iniciar o Detener. Si ve agentes, seleccione cualquier agente y haga clic en Reiniciar.

Creación de grupos de agentes

Puede crear un grupo de agentes para organizar los agentes por ubicación, sistema operativo o cualquier otra categoría que considere oportuna. El proceso de creación de un grupo de agentes mediante el asistente para grupos de agentes consta de los pasos siguientes:

1. Apertura del asistente para grupos de agentes.
2. Introducción de detalles del grupo.
3. Adición de agentes.

Más información

[Apertura del asistente para grupos de agentes](#) (en la página 677)

[Adición de detalles a grupos de agentes](#) (en la página 678)

Apertura del asistente para grupos de agentes

Para crear un grupo de agentes nuevo o editar uno existente, abra el asistente para grupos de agentes.

Para abrir el asistente para grupos de agentes

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.
Aparece la lista de la carpeta Recopilación de registros.
2. Haga clic en la carpeta Explorador de agentes.
Los botones de la gestión de agentes aparecerá en el panel de detalles.
3. Haga clic en Nuevo grupo de agentes: 
Aparece el asistente para grupos de agentes.
Al emplear el asistente:
 - Haga clic en Guardar para guardar el archivo sin cerrar el asistente.
 - Haga clic en Guardar y cerrar para guardar el archivo y cerrar el asistente.
 - Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Adición de detalles a grupos de agentes

Puede agregar detalles identificativos al grupo de agentes.

Para agregar detalles a grupos de agentes

1. Abra el Asistente para grupos de agentes.
2. Introduzca un nombre para el grupo y una descripción opcional como referencia.
3. Seleccione el modo de envío de eventos.
4. (Opcional) Introduzca los primeros caracteres del servidor que desea agregar en el campo Patrón de nombre.

En el área Disponible, aparecerán los servidores que coincidan con la búsqueda.

5. Seleccione los servidores que desea agregar mediante el control de cambio, y ordénelos como desee que aparezcan en la pantalla del grupo de agentes mediante las flechas de dirección.
6. Vaya al paso siguiente o haga clic en Guardar y cerrar.

Si hace clic en Guardar y cerrar, se crea el grupo; si no es así, aparece el paso que haya seleccionado.

Adición de agentes a grupos de agentes

Puede agregar agentes a los grupos de agentes con fines administrativos. Por ejemplo, puede crear grupos por región geográfica o sistema operativo.

Nota: Las propiedades de un grupo de agentes se aplican a todos los agentes dentro del mismo.

Para agregar agentes a grupos

1. Abra el Asistente de grupos de agentes y vaya al paso Agentes.
2. (Opcional) Seleccione los criterios de búsqueda de agentes. Si no introduce términos de búsqueda, aparecen todos los agentes. Se pueden seleccionar uno o más de los siguientes criterios para limitar la búsqueda:
 - Grupo de agentes: sólo devuelve los agentes asignados al grupo seleccionado
 - Plataforma: sólo devuelve los agentes que se ejecutan en la plataforma seleccionada
 - Patrón del nombre de agente: sólo devuelve los agentes que contienen el patrón especificado
3. Haga clic en Buscar.

Los agentes que coinciden con la búsqueda aparecen en el área Agentes disponibles.
4. Seleccione los agentes que desea agregar mediante el control de cambio, y ordénelos de la forma en la que desea que aparezcan en la pantalla del grupo de agentes mediante las flechas de dirección.

Nota: No se puede mover un agente a un grupo de agentes que no tenga configurados los servidores de CA Enterprise Log Manager.
5. Haga clic en Guardar y cerrar.

El grupo de agentes aparece en la lista.

Nota: Si se suprime un grupo de agentes creado por el usuario, los agentes del grupo de agentes se mueven al grupo de agentes predeterminado, y los agentes heredan las propiedades del mismo.

Configuración de la gestión de agentes

Puede configurar que los agentes o los grupos de agentes envíen informes a distintos servidores de CA Enterprise Log Manager del entorno federado. Esto le permite establecer que los grupos o agentes envíen información de eventos a servidores de CA Enterprise Log Manager seleccionados.

El proceso de configuración de la gestión de agentes mediante el asistente de servidores del gestor de registros consta de los pasos siguientes:

1. Apertura del asistente de asignación de servidores del gestor de registros.
2. Selección de los destinos de grupos de agentes que se van a asignar.
3. Selección de los servidores de CA Enterprise Log Manager a los que se van a asignar agentes o grupos.

Más información

[Apertura del asistente de asignación de servidores del gestor de registros](#) (en la página 681)

[Selección de agentes de destino](#) (en la página 682)

[Selección de gestores de registros](#) (en la página 683)

Apertura del asistente de asignación de servidores del gestor de registros

Para configurar las asignaciones de agentes o grupos de agentes, abra el asistente de asignación de servidores del gestor de registros.

Para abrir el asistente de asignación de servidores del gestor de registros

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de carpetas de recopilación de registros, que muestra los botones de gestión de agentes en el panel de detalles.

2. Haga clic en Servidores del gestor de registros: 

Aparece el asistente de asignación de servidores del gestor de registros.

Al emplear el asistente:

- Haga clic en Guardar para guardar sin cerrar el asistente.
- Haga clic en Guardar y Cerrar para guardar la asignación y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Más información

[Configuración de la gestión de agentes](#) (en la página 680)

[Selección de agentes de destino](#) (en la página 682)

[Selección de gestores de registros](#) (en la página 683)

Selección de agentes de destino

Para asignar agentes a un servidor con fines de recepción de eventos y almacenamiento, debe seleccionar el agente o el grupo que desea asignar a un determinado servidor de CA Enterprise Log Manager.

Para seleccionar agentes de destino

1. Abra el asistente de asignación de servidores del gestor de registros.
2. Seleccione si desea asignar los agentes por grupos o de forma individual.
3. Si prefiere hacerlo por grupos, utilice el control de cambio para seleccionar los grupos que desea asignar. Puede emplear el campo de introducción de búsqueda para ubicar los grupos introduciendo un nombre parcial. Los grupos disponibles se filtran según escribe.
4. Si prefiere hacerlo por agentes, utilice el control de cambio para seleccionar los agentes individuales que desea asignar. Puede emplear las listas desplegables Grupo de agentes y Plataforma, y el campo de introducción de búsquedas para localizar los agentes.
5. Vaya al paso de selección del gestor de registros.

Más información

[Configuración de la gestión de agentes](#) (en la página 680)

[Apertura del asistente de asignación de servidores del gestor de registros](#) (en la página 681)

[Selección de gestores de registros](#) (en la página 683)

Selección de gestores de registros

Seleccione el servidor de CA Enterprise Log Manager al que desea asignar agentes o grupos de agentes.

Para seleccionar servidores de gestores de registros

1. Abra al asistente de asignación de servidores del gestor de registros, seleccione los agentes de destino y vaya al paso de selección de gestores de registros.
2. Utilice el control de cambio para seleccionar los servidores a los que va a asignar agentes o grupos de agentes. Puede emplear el campo de entrada Patrón de nombre para buscar la lista disponible.
3. Haga clic en Guardar y cerrar.

Los agentes o los agentes agrupados se asignan a los servidores seleccionados.

Más información

[Configuración de la gestión de agentes](#) (en la página 680)

[Apertura del asistente de asignación de servidores del gestor de registros](#) (en la página 681)

[Selección de agentes de destino](#) (en la página 682)

Protección de los agentes contra el impacto de los cambios de dirección IP del servidor

Al instalar un agente, asigna un servidor de CA Enterprise Log Manager principal para que el agente se ponga en contacto en primer lugar con los eventos recopilados. Al configurar un agente, agregue otros servidores de CA Enterprise Log Manager en una lista ordenada. Cuando un agente que está listo para enviar registros recopilados al servidor principal no es capaz de contactar con él, dicho agente se pone en contacto con cada servidor secundario de la lista hasta que encuentra uno disponible. La configuración de una lista ordenada de servidores secundarios garantiza el envío de registros del agente al servidor. Un agente sólo puede enviar eventos a un servidor de CA Enterprise Log Manager cada vez; es decir, no se produce una duplicación de eventos.

Cuando los servidores seleccionados para gestionar un agente cambian de dirección IP, puede verse afectada la capacidad del agente para transferir eventos recopilados a un servidor de su lista. Al llevar a cabo pasos como medidas de precaución, puede asegurarse de que los servidores sigan estando muy disponibles para los agentes que los emplean, incluso en el caso de que dichos servidores sufran reasignaciones manuales o dinámicas de sus direcciones IP.

La dirección IP de un servidor de CA Enterprise Log Manager instalado podría cambiar en los casos siguientes:

- Reasignación dinámica mediante DHCP

El servidor de CA Enterprise Log Manager de un sistema de servidor único se configura para que el DHCP asigne sus direcciones IP. En algún momento después de haber seleccionado este servidor para gestionar agentes, el DHCP le asigna una dirección IP nueva. Esto puede ocurrir cuando el servidor de CA Enterprise Log Manager está desconectado el tiempo suficiente como para que finalice el arrendamiento de la dirección IP. No es necesaria ninguna notificación al usuario cuando se cambian direcciones IP de forma dinámica.

- Reasignación manual

Los servidores de CA Enterprise Log Manager se configuran con direcciones IP estáticas. En el caso de un proceso del sitio en el que las direcciones IP se reasignan como parte de la implementación de una subred nueva, se asignan direcciones IP nuevas de forma manual a los servidores de CA Enterprise Log Manager.

Lleve a cabo la acción adecuada para asegurar una alta disponibilidad de servidores para agentes si las direcciones IP de dichos servidores podrían cambiar.

Más información:

[Disponibilidad de servidores con direcciones IP dinámicas](#) (en la página 685)
[Disponibilidad de servidores durante la reasignación de direcciones IP estáticas](#) (en la página 685)

Disponibilidad de servidores con direcciones IP dinámicas

Si selecciona un DHCP al instalar un servidor de CA Enterprise Log Manager único, especifique el nombre de host (no la dirección IP) de dicho servidor de CA Enterprise Log Manager al instalar cada agente. Esto garantizará que las reasignaciones de DHCP de la dirección IP del servidor de CA Enterprise Log Manager no afectarán a los agentes que lo utilizan.

Si especifica la dirección IP del servidor de CA Enterprise Log Manager al instalar los agentes y dicha dirección IP cambia, tendrá que volver a instalar los agentes para restablecer la disponibilidad del servidor de CA Enterprise Log Manager único. Para evitar este posible problema, es recomendable que instale otro servidor de CA Enterprise Log Manager y que lo añada como servidor secundario a todos los agentes. Esto garantizará una alta disponibilidad de los servidores.

Disponibilidad de servidores durante la reasignación de direcciones IP estáticas

Si instala los servidores de CA Enterprise Log Manager con direcciones IP estáticas y luego pretende volver a numerarlos, utilice el flujo de trabajo siguiente para garantizar una alta disponibilidad ininterrumpida para los agentes que tengan estos servidores en sus listas ordenadas. No es necesario reiniciar el agente tras cada paso, ya que el agente actualiza la información de configuración cada 5 minutos de forma predeterminada.

Importante: Si el agente sólo se ha configurado con un servidor de CA Enterprise Log Manager en un sistema con múltiples servidores, asegúrese de añadir un segundo servidor a la lista ordenada antes de asignar direcciones IP nuevas. Si no lo hace, puede que tenga que volver a instalar y configurar el agente tras la asignación de direcciones IP del servidor para restablecer la disponibilidad del servidor.

Para asegurarse de que los agentes puedan comunicarse con un servidor de CA Enterprise Log Manager de su lista ordenada durante una reasignación de direcciones IP estáticas en los servidores

1. Si pretende reasignar direcciones IP en un servidor de CA Enterprise Log Manager que es el único servidor de CA Enterprise Log Manager, instale un servidor de CA Enterprise Log Manager temporal que señale a CA EEM en el servidor de CA Enterprise Log Manager original.
2. Si no se han configurado uno o varios servidores de CA Enterprise Log Manager más para los agentes de un sistema con múltiples servidores, asigne al menos un servidor más a la lista ordenada.
 - a. Seleccione Explorador de agentes y haga clic en Servidores del gestor de registros.

Aparece el asistente de asignación de servidores del gestor de registros y muestra el paso de selección de destinos.
 - b. Seleccione Agentes o Grupos en función del modo de realización de las asignaciones.
 - c. Seleccione los agentes o grupos correspondientes como destinos en la lista Disponible y trasládelos a la lista Seleccionado.
 - d. Haga clic en el paso de selección de servidores del gestor de registros.
 - e. Seleccione un CA Enterprise Log Manager en la lista Disponible y trasládelo a la lista Seleccionado.
 - f. Haga clic en Guardar y cerrar.
3. Elimine la mitad de la lista ordenada de servidores de CA Enterprise Log Manager de la configuración del agente o del grupo de agentes mediante el asistente de asignación de servidores del gestor de registros.
4. Asigne las nuevas direcciones IP estáticas a los servidores eliminados de la lista seleccionada.
5. Vuelva a añadir los servidores con las direcciones IP nuevas.
6. Espere a que el agente actualice la información de configuración.

Nota: Puede reiniciar el agente de forma manual para actualizar la información de manera inmediata.
7. Elimine la otra mitad de la lista ordenada.

Nota: En el caso de que haya añadido un servidor temporal, puede mantenerlo para acciones de conmutación o puede desinstalarlo y, a continuación, eliminarlo.

8. Reasigne las direcciones IP correspondientes.
9. Vuelva a añadir esos servidores para restablecer la lista ordenada original.

Más información:

[Configuración de la gestión de agentes](#) (en la página 680)

[Eliminación de hosts de servicio](#) (en la página 153)

Aplicación de actualizaciones de suscripción

Puede aplicar actualizaciones de suscripción de CA a agentes o conectores. El proceso de aplicación de paquetes de suscripción mediante el asistente de listas de actualizaciones consta de los pasos siguientes:

1. Apertura del asistente de listas de actualizaciones
 2. Selección de uno de los tipos de actualizaciones siguientes y especificación de criterios de búsqueda para paquetes de actualizaciones disponibles:
 - Actualizaciones de agentes
 - Actualizaciones de integraciones para conectores
- Nota:** Si hay actualizaciones de agentes y conectores, debe aplicar las actualizaciones de agentes en primer lugar para que la actualización se realice de forma adecuada.
3. Selección de agentes o conectores para actualizarlos a la versión más reciente

Más información

[Apertura del asistente de listas de actualizaciones](#) (en la página 688)

[Selección de los agentes o conectores que se van a actualizar](#) (en la página 689)

[Actualización de versiones de integración de agentes o conectores](#) (en la página 690)

Apertura del asistente de listas de actualizaciones

Para actualizar agentes o conectores a la versión más reciente, abra el asistente de listas de actualizaciones.

Para abrir del asistente de listas de actualizaciones

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

Aparece la lista de la carpeta Recopilación de registros.

2. Haga clic en la carpeta Explorador de agentes.

Los botones de gestión de agentes aparecen en el panel de detalles.

3. Haga clic en Suscripción: 

Aparece el asistente de listas de actualizaciones.

Al emplear el asistente:

- Haga clic en Guardar para guardar sin cerrar el asistente.
- Haga clic en Guardar y cerrar para guardar el progreso y cerrar el asistente.
- Haga clic en Restablecer para volver a mostrar en la pantalla del asistente la configuración guardada más recientemente.

Selección de los agentes o conectores que se van a actualizar

Puede comprobar si hay actualizaciones disponibles mediante la especificación de los criterios de búsqueda de los agentes o conectores correspondientes.

Para seleccionar los agentes o conectores que se van a actualizar

1. Abra el asistente de listas de actualizaciones.
Aparece la lista de selección de actualizaciones.
2. Seleccione Actualizaciones del agente o Actualizaciones del conector.
Nota: Si hay actualizaciones de agentes y conectores, debe aplicar las actualizaciones de agentes en primer lugar para que la actualización se realice de forma adecuada.
3. Siga estas indicaciones para establecer los criterios de búsqueda de la actualización del agente o conector:
 - a. Seleccione un grupo de agentes en la lista desplegable.
 - b. Seleccione la plataforma en la lista desplegable.
 - c. Indique el patrón de nombres de agentes mediante comodines.
 - d. (Sólo en el caso de actualizaciones de integración del conector)
Seleccione Integración en la lista desplegable.
4. Haga clic en Buscar.
Los paquetes de actualización que coincidan con los criterios de búsqueda aparecen en el siguiente paso del asistente, relativo a la selección de versiones. Debe avanzar al paso de selección de versiones para visualizarlos y aplicarlos.

Más información:

[Apertura del asistente de listas de actualizaciones](#) (en la página 688)

[Actualización de versiones de integración de agentes o conectores](#) (en la página 690)

Actualización de versiones de integración de agentes o conectores

Puede comparar la versión de cada agente o conector listado con las versiones de actualizaciones descargadas para determinar si es necesaria una actualización y, a continuación, especifique si desea sustituir la versión actual por una versión diferente.

Para actualizar agentes o conectores

1. Abra el asistente de listas de actualizaciones y seleccione los agentes o conectores que desee tener en cuenta para la actualización.

2. Vaya al paso de selección de versiones.

Aparece la lista de agentes o conectores que cumplen los criterios de búsqueda.

- Cada agente se muestra con la versión actual y una lista desplegable que muestra las versiones de las actualizaciones disponibles.
- Cada conector se muestra con la versión de integración actual y una lista desplegable que muestra las versiones de las actualizaciones disponibles.

3. (Opcional) Seleccione Omitir versión de sistema operativo para ver todas las actualizaciones disponibles para el sistema operativo seleccionado independientemente de la versión.
4. Seleccione los agentes o conectores a los que desea aplicar las actualizaciones y haga clic en Guardar y cerrar.

El agente instala las actualizaciones y sustituye la versión actual por la actualización de la integración o del agente seleccionado.

Nota: Puede comprobar si todos los agentes o conectores cuentan con la versión más reciente mediante la revisión de estos detalles tras aplicar las actualizaciones seleccionadas.

Creación de un archivo de diagnóstico del agente para el Departamento de Soporte Técnico.

Se pueden revisar los archivos de registro y de configuración de un agente de CA Enterprise Log Manager seleccionado. La herramienta AgentDiagnostics empaqueta la información del sistema y los archivos de registro en un archivo .tar comprimido para transmitirlos al personal del Departamento de Soporte Técnico de CA Technologies. Para transferir este archivo puede utilizarse FTP o cualquier otro método de transferencia de archivos.

Nota: Parte de la información del archivo resultante puede ser confidencial como, por ejemplo, las direcciones IP, las configuraciones del sistema, los registros del hardware y los registros de procesos. Utilice un método seguro para almacenar y transportar este archivo.

Para crear un archivo de diagnóstico del agente

1. Vaya al directorio bin del agente de CA Enterprise Log Manager.

Ruta predeterminada en Windows: C:\Archivos de programa\CA\elmagent\bin

Ruta predeterminada en UNIX/Linux: /opt/CA/ELMagent/bin

2. Realice *uno* de los siguientes pasos:
 - a. Si está ejecutando el agente en un sistema Windows, ejecute el archivo AgentDiagnostics.bat.
 - b. Si está ejecutando el agente en un sistema UNIX/Linux, ejecute el archivo AgentDiagnostics.sh.

Se crea un archivo de diagnóstico del agente con el formato de archivo *agenthostname_DDMMYYYY_HHMM.tar.gz*.

Capítulo 21: Certificados personalizados

Esta sección contiene los siguientes temas:

[Implementación de certificados personalizados](#) (en la página 693)

[Adición del certificado de raíz de confianza al servidor de gestión de](#)

[CA Enterprise Log Manager](#) (en la página 694)

[Adición de certificados de raíz de confianza para todos los demás servidores de](#)

[CA Enterprise Log Manager](#) (en la página 696)

[Adición del nombre común del certificado a una política de acceso](#) (en la página 697)

[Implementación de certificados nuevos](#) (en la página 698)

Implementación de certificados personalizados

El proceso de instalación genera dos certificados y los coloca en el directorio `/opt/CA/SharedComponents/iTechnology` del servidor de CA Enterprise Log Manager. Puede emplear los certificados instalados sin modificarlos. Estos certificados tienen los nombres siguientes, donde *ApplicationName* es CAELM para el producto CA Enterprise Log Manager.

- *ApplicationNameCert.cer*

Este certificado lo emplean todos los servicios de CA Enterprise Log Manager para comunicarse con el servidor de gestión. La entrada de este certificado también se encuentra en el archivo `CALM.cnf`.

- *ApplicationName_AgentCert.cer*

Este certificado lo emplean todos los agentes para comunicarse con el servidor de CA Enterprise Log Manager.

Importante: Para sustituir el certificado `CAELM_AgentCert.cer` por un certificado personalizado en un entorno que disponga de agentes activos es necesario volver a instalar los agentes.

Antes de poder utilizar certificados personalizados es necesario obtener un certificado de raíz de confianza de una autoridad emisora de certificados raíz (CA). Una autoridad certificadora puede emitir varios certificados en forma de estructura de árbol. Todos los certificados dependientes del certificado raíz de confianza heredan la confianza del certificado raíz. Este proceso presupone que, si se sustituyen ambos certificados, el certificado de servicio personalizado y el certificado de agente personalizado utilizan la misma raíz de confianza.

Sólo se admiten certificados personalizados con extensiones .cer. Tras obtener un certificado raíz de confianza, la secuencia de acciones habitual para implementar certificados personalizados es la siguiente:

1. Agregar el certificado de raíz de confianza a iAuthority.conf en el servidor de gestión de CA Enterprise Log Manager o en el servidor independiente de CA EEM.
2. Si se sustituye CAELM_AgentCert.cer, se debe agregar el certificado de raíz de confianza a iControl.conf en el servidor de gestión de CA Enterprise Log Manager, y a continuación repetir esta acción en cada servidor de CA Enterprise Log Manager.
3. Si se sustituye CAELMCert.cer, se debe agregar el nombre común de este certificado personalizado en la política de alcance AdministerObjects en el servidor de gestión CA Enterprise Log Manager o el servidor independiente CA EEM.
4. Agregue los certificados personalizados a la carpeta de iTechnology de cada servidor de CA Enterprise Log Manager y agregue el nombre y contraseña para cada certificado en archivos de configuración separados.

Adición del certificado de raíz de confianza al servidor de gestión de CA Enterprise Log Manager

En primer lugar, es necesario obtener un certificado raíz de confianza en formato PEM de la autoridad de certificación (CA). A continuación, se debe agregar este certificado de raíz de confianza al interfaz Web del SPIN de iTechnology del servidor de gestión o el servidor independiente de CA EEM.

Para agregar el certificado de raíz de confianza al servidor de gestión de CA Enterprise Log Manager

1. Desplácese hasta la interfaz Web del SPIN de iTechnology de CA para servidor de gestión de CA Enterprise Log Manager o el servidor independiente de CA EEM.

`https://<management_ELM_hostname>:5250/spin`

`https://<EEM_hostname>5250/spin`

Aparece la página de SPIN de iTechnology de CA.

2. Seleccione iTech Administrator en la lista desplegable y haga clic en Go.

La página Administrador de iTechnology aparece con un vínculo de inicio de sesión.

3. Haga clic en Inicio de sesión.

Aparecerá el cuadro de diálogo de inicio de sesión de iTechnology de CA.

4. Introduzca las credenciales EiamAdmin, seleccione iAuthority y haga clic en Inicio de sesión.

5. Seleccione la ficha iAuthority y agregue la raíz de confianza a iAuthority.conf de la manera siguiente:

- a. Introduzca una etiqueta para el certificado. No introduzca "yo" como la etiqueta.
- b. Busque y seleccione el archivo .cer.
- c. Haga clic en la opción de adición de raíz de confianza.

El mensaje de confirmación indica que la raíz de confianza se agrega a iAuthority.conf, un archivo que existe solamente en el servidor de gestión o en el servidor independiente de CA EEM.

6. Si utiliza un servidor CA EEM independiente, avance hasta el último paso.

7. Si se sustituye el certificado CAELM_AgentCert.cer con un certificado personalizado, se debe agregar la raíz de confianza a iControl.conf de la forma siguiente:

- a. Seleccione la ficha Configurar.
- b. Para el certificado, introduzca la misma etiqueta que haya introducido en el paso anterior.
- c. Busque y seleccione el mismo archivo PEM de raíz (.cer) que se ha seleccionado en el paso anterior.
- d. Haga clic en la opción de adición de raíz de confianza.

El mensaje de confirmación indica que la raíz de confianza del certificado personalizado se agrega al archivo iControl.conf en el directorio iTechnology del servidor de gestión de CA Enterprise Log Manager.

8. Haga clic en el botón de cierre de sesión y cierre SPIN de iTechnology.

Adición de certificados de raíz de confianza para todos los demás servidores de CA Enterprise Log Manager

Si se reemplaza el certificado CAELM_AgentCert.cer con un certificado personalizado, se puede agregar el certificado de raíz de confianza a la interfaz Web del SPIN de iTechnology de cada servidor adicional de CA Enterprise Log Manager. En este procedimiento, se agrega el certificado de raíz de confianza a iControl de CA. Este procedimiento no es necesario si sólo se está sustituyendo el certificado CAELMCert.cer.

Para agregar el certificado de raíz de confianza a iControl de CA en cada servidor de CA Enterprise Log Manager que no se de gestión

1. Inicie sesión en la interfaz de usuario de SPIN en el iGateway donde se ejecuta el servidor que no es de gestión. Utilice la URL siguiente:
`https://<ELM_hostname>:5250/spin/`
Aparece la página de SPIN de iTechnology de CA.
2. Seleccione iTech Administrator en la lista desplegable y haga clic en Go.
La página Administrador de iTechnology aparece con un vínculo de inicio de sesión.
3. Haga clic en Inicio de sesión.
Aparecerá el cuadro de diálogo de inicio de sesión de iTechnology de CA.
4. Introduzca las credenciales EiamAdmin, seleccione iAuthority y haga clic en Inicio de sesión.
5. Seleccione la ficha Configurar y agregue la raíz de confianza de la forma siguiente:
 - a. Para el certificado, introduzca la misma etiqueta que haya introducido en el paso anterior.
 - b. Busque y seleccione el archivo .cer.
 - c. Haga clic en la opción de adición de raíz de confianza.La raíz de confianza del certificado personalizado se agrega al archivo iControl.conf en el directorio iTechnology. Aparecerá un mensaje de confirmación.
6. Haga clic en el botón de cierre de sesión y cierre SPIN de iTechnology.

Adición del nombre común del certificado a una política de acceso

Todos los servicios de CA Enterprise Log Manager utilizan el certificado CAELMCert.cer para comunicarse con el servidor de gestión de CA Enterprise Log Manager. Si se sustituye CAELMCert.cer con un certificado personalizado, se debe agregar el nombre común (cn) de este certificado personalizado a la política AdministerObjects en el servidor de gestión o en el servidor independiente de CA EEM.

Nota: No es necesario suprimir la identidad [User] CERT_CAELM, el nombre común del certificado predeterminado, de esta política.

Para agregar el nombre común del certificado personalizado a la política AdministerObjects

1. Para desplazarse hasta el servidor de gestión de CA Enterprise Log Manager o el servidor independiente de CA EEM, introduzca la URL adecuada.

`https://<management_server_hostname>:5250/spin/cal`

`https://<EEM_server_hostname>:5250/spin/eiam`

2. Inicie sesión con privilegios administrativos en el servidor de gestión de CA Enterprise Log Manager. Si está accediendo a un servidor CA EEM, debe iniciar sesión como el usuario EiamAdmin.
3. Haga clic en la ficha Administración, acceda a la subficha Gestión de usuarios y accesos y finalmente haga clic en el vínculo Política de acceso, en el panel izquierdo. Si está conectado a un servidor independiente de CA EEM, haga clic en la ficha Gestionar políticas de acceso.
4. Haga clic en el vínculo de políticas de ámbito.

Aparece la tabla de políticas de las políticas de ámbito en el panel principal.

5. Desplácese hasta la política AdministerObjects y seleccione el vínculo AdministerObjects.

La política AdministerObjects se abre en modo de edición.

6. Agregue el nombre común (cn) del certificado personalizado de la forma siguiente:

- a. Introduzca el nombre común del certificado personalizado en el campo Identidad.

- b. Haga clic en la flecha para desplazar la introducción.

[User]<custom certificate cn> aparece en la lista Identidades seleccionadas.

7. Haga clic en Save.

La política AdministerObjects se guarda con la adición del nombre común del certificado personalizado como identidad que tiene acceso de lectura y escritura a los recursos listados en esta política.

8. Haga clic en Cerrar y cierre la sesión de la interfaz de usuario de CA Enterprise Log Manager.

Implementación de certificados nuevos

CA Enterprise Log Manager emplea dos certificados. Se pueden sustituir uno o los dos certificados predefinidos por certificados personalizados. Para implementar certificados nuevos, inicie sesión en el dispositivo de software, detenga iGateway, agregue los certificados nuevos, modifique los archivos de configuración respectivos y, a continuación, reinicie iGateway.

Antes de implementar certificados nuevos, compruebe lo siguiente:

- El certificado de raíz de confianza se ha agregado a iTechnology iAuthority en el servidor de gestión o el servidor independiente de CA EEM que utilizan los servidores de CA Enterprise Log Manager.
- Si está sustituyendo CAELM_AgentCert.cer con un certificado personalizado, se debe haber agregado el certificado de raíz personalizado al archivo iControl en iTechnology de cada servidor CA Enterprise Log Manager.
- El nombre común del certificado personalizado se ha añadido a la política de acceso AdministerObjects. Esto hace referencia al certificado personalizado que va a sustituir CAELMCert.cer.

Para implementar certificados nuevos

1. Acceda al host donde está instalado el servidor CA Enterprise Log Manager.
2. Utilice las credenciales de **caelmadmin** para registrarse en el servidor de CA Enterprise Log Manager.
3. Al solicitársele, dirija a los usuarios a la raíz, es decir:

su - root
4. Cambie los directorios a /opt/CA/SharedComponents/iTechnology mediante el atajo siguiente:

```
cd $IGW_LOC
```

5. Detenga iGateway:

```
./S99igateway stop
```

6. Para reemplazar CAELMCert.cer:

- a. Copie el certificado personalizado *ApplicationNameCert.cer* y el archivo de clave *ApplicationNameCert.key* en el directorio iTechnology.
- b. Abra el archivo CALM.cnf. Sustituya el nombre del certificado por el nombre nuevo.
- c. Sustituya el nombre del archivo de clave existente con el nuevo nombre del archivo de clave.

7. Para sustituir CAELM_AgentCert.cer:

- a. Copie el certificado personalizado *ApplicationName_AgentCert.cer* y el archivo de clave *ApplicationName_AgentCert.key* en el directorio iTechnology.
- b. Abra el archivo AgentManager.conf. Sustituya el nombre del certificado por el nombre nuevo.
- c. Sustituya el nombre del archivo de clave existente con el nuevo nombre del archivo de clave.

8. Inicie iGateway.

```
./S99igateway start
```

Si se sustituye CAELM_AgentCert.cer, todos los agentes instalados después de esta implementación automáticamente utilizarán el certificado personalizado.

Apéndice A: Funcionalidades de accesibilidad

CA se compromete a garantizar que todos los clientes, independientemente de su capacidad, puedan emplear correctamente los productos y la documentación compatible para llevar a cabo las tareas de negocio vitales. Esta sección explica las funciones de accesibilidad que forman parte de CA Enterprise Log Manager.

Modo de accesibilidad

Puede configurar CA Enterprise Log Manager para emplear un modo de accesibilidad que muestre todos los paneles gráficos de consultas e informes en forma de tablas. Para acceder al modo de accesibilidad, seleccione la casilla de verificación Activar accesibilidad en la pantalla de inicio de sesión.

Controles de accesibilidad

Puede emplear los controles del teclado para navegar por CA Enterprise Log Manager, tal y como se indica en la tabla siguiente:

Tareas	Controles del teclado
Alternancia entre aplicaciones abiertas	CTRL-TAB
Selección de un archivo en una ventana abierta	CTRL-TAB
Ayuda	F1
Clic en botón	Barra espaciadora o Intro
Selección de casilla de verificación	Barra espaciadora o Intro
Apertura de menú, cuadro combinado	CTRL + Flecha hacia abajo
Navegación por una lista	CTRL + Flecha hacia abajo para resaltar Flechas hacia arriba/abajo para navegar Barra espaciadora o Intro para seleccionar un elemento de la lista

Tareas	Controles del teclado
Grupo de botones de opción	CTRL + Flecha hacia abajo para resaltar Flechas hacia arriba/abajo para navegar Barra espaciadora o Intro para seleccionar un elemento de la lista
Cierre de la ventana activa	ALT-F4
Doble clic	CTRL + D

Configuración de idiomas en CA Enterprise Log Manager

Puede visualizar la interfaz de CA Enterprise Log Manager en los idiomas siguientes, aparte del inglés:

- Francés
- Italiano
- Alemán
- Español
- Japonés

Modifique la configuración de idioma en la ventana del explorador. Por ejemplo, si utiliza Microsoft Internet Explorer, abra el cuadro de diálogo Opciones de Internet y agregue o seleccione el idioma principal que desea visualizar.

Si selecciona uno de los cinco idiomas soportados, la interfaz de CA Enterprise Log Manager se muestra en el idioma correspondiente. Las etiquetas y las fichas de la interfaz están traducidas, pero algunos elementos no lo están: por ejemplo, los títulos de las etiquetas y las cadenas de datos de los resultados de los informes se han dejado en inglés.

Nota: Si visualiza CA Enterprise Log Manager al realizar un cambio de idioma, actualice la ventana del explorador para ver el idioma nuevo. Si ha iniciado sesión al realizar el cambio, se vuelve a mostrar la pantalla de inicio de sesión en el idioma nuevo.

Localización manual de CA Enterprise Log Manager

Puede localizar manualmente CA Enterprise Log Manager mediante la creación de sus propios archivos de idioma. De esta forma, puede ver la interfaz de CA Enterprise Log Manager en otros idiomas diferentes de los que ya se admiten. Puede hacerlo mediante la copia de los archivos existentes que puede utilizar como plantillas.

Para localizar CA Enterprise Log Manager manualmente

1. Inicie sesión en su host de servidor de CA Enterprise Log Manager, desplácese a `opt/CA/LogManager/local` y seleccione los archivos que desee utilizar como plantillas. Existen dos archivos para cada idioma:
 - `content.properties`: contiene texto que describe diferentes contenidos, como nombres de consultas e informes, y descripciones.
 - `ui.properties`: contiene cadenas de texto para títulos de funciones, como etiquetas de fichas y encabezados.

Cada archivo va precedido de un prefijo de idioma estándar. Por ejemplo, el archivo de contenido en alemán se denomina `de_content.properties`. El archivo de interfaz en inglés se denomina `en_ui.properties`.

2. Copie uno de cada tipo de archivo y cámbieles el nombre con el prefijo estándar. Por ejemplo, si desea crear un archivo de localización para portugués, deberá copiar los archivos y cambiarles el nombre a `pt_content.properties` y `pt_ui.properties`.

Nota: Los prefijos de idioma se pueden encontrar en la lista de idiomas compatibles de su explorador.

3. Abra los archivos y traduzca las cadenas en el idioma original al idioma que desee. Por ejemplo, si ha copiado los archivos en inglés, debe sustituir todas las cadenas de texto en inglés por el idioma deseado.
4. Guarde los archivos traducidos manualmente en la ubicación indicada en el paso 1, en todos los servidores de CA Enterprise Log Manager en los que desee que se encuentren disponibles.
5. Establezca el explorador en el idioma de destino e inicie sesión en CA Enterprise Log Manager.

Más información:

[Configuración de idiomas en CA Enterprise Log Manager](#) (en la página 702)

Apéndice B: Acceso a eventos recopilados con ODBC y JDBC

Esta sección contiene los siguientes temas:

[Acerca del acceso mediante ODBC/JDBC en CA Enterprise Log Manager](#) (en la página 705)

[Creación de consultas relativas a ODBC y JDBC para el uso con CA Enterprise Log Manager](#) (en la página 706)

[Procesamiento de las consultas](#) (en la página 708)

[Ejemplo: Empleo de un filtro de acceso para limitar los resultados de ODBC](#) (en la página 710)

[Ejemplo: Preparación para el uso de clientes de ODBC y JDBC con Crystal Reports](#) (en la página 712)

[Uso de Crystal Reports para acceder al almacén de registro de eventos con ODBC](#) (en la página 720)

[Acceso a eventos desde Crystal Reports con JDBC](#) (en la página 721)

[Supresión del cliente de ODBC en sistemas Windows](#) (en la página 723)

[Supresión de clientes de JDBC](#) (en la página 723)

Acerca del acceso mediante ODBC/JDBC en CA Enterprise Log Manager

CA Enterprise Log Manager ofrece un acceso de ODBC y JDBC de sólo lectura al almacén de registro de eventos para permitirle llevar a cabo las acciones siguientes:

- Configurar informes personalizados con una utilidad de generación de informes externa, como BusinessObjects Crystal Reports
- Recuperar información de registros seleccionados mediante aplicaciones externas

Estas funciones le permiten crear y dar forma a sus propios informes personalizados mediante información de registro que ya ha sido recuperada por CA Enterprise Log Manager. Además, puede recuperar datos para su uso en los equipos de correlación existentes, en los paquetes de detección de software maligno y en otras funciones.

Tras instalar el cliente suministrado por CA en el sistema que desea emplear para acceder al almacén de registro de eventos, configure una conexión al origen de datos y, a continuación, comience a recuperar datos. El servicio de suscripción instala los componentes del servidor.

Creación de consultas relativas a ODBC y JDBC para el uso con CA Enterprise Log Manager

La compatibilidad con ODBC y JDBC en CA Enterprise Log Manager se limita a consultas de sólo lectura mediante instrucciones SELECT en las tablas siguientes.

- VIEW_EVENT: contiene eventos de la base de datos de evento.
- VIEW_INCIDENT: contiene incidentes de la base de datos de incidentes.
- VIEW_INCIDENTEVENT_BYID: contiene eventos componentes de incidentes de la base de datos de eventos de incidente.

Cree instrucciones SELECT mediante reglas y formatos ANSI SQL. Los componentes del servidor contienen un motor de análisis de SQL. El analizador implementa una gran parte de SQL de nivel de entrada tal y como se define en la especificación X3.135-1992, "SQL de idioma de base de datos". El analizador también soporta funciones SQL de ANSI SQL99 y bases de datos comerciales como Microsoft SQL Server y Oracle. El analizador cumple con la especificación de gramática mínima de ODBC.

La gramática de eventos comunes sirve como esquema para esta tabla. Consulte la *Guía de referencia de la gramática de eventos comunes* para obtener detalles sobre el esquema.

Limitaciones de soporte de SQL

CA Enterprise Log Manager no soporta llamadas de procedimientos almacenados, comandos de lenguaje de control de datos (DCL) ni comandos de lenguaje de definición de datos (DDL).

CA Enterprise Log Manager no soporta las siguientes palabras clave y operaciones de lenguaje de manipulación de datos (DML):

- UNION
- JOIN
- Nested SELECT

- INSERT
- UPDATE
- DELETE
- Operadores de control de transacciones, como COMMIT, ROLLBACK, etc.

Funciones SQL compatibles

A continuación, se indican las funciones SQL compatibles para su empleo en la creación de instrucciones SELECT:

- *ABS(numeric_exp)*
- *ROUND(numeric_exp, integer_exp)*
- *LCASE(string_exp)*
- *LOWER(string_exp)*
- *LENGTH(string_exp)*
- *LTRIM(string_exp)*
- *RTRIM(string_exp)*
- *SUBSTRING(string_exp, start, length)*
- *UCASE(string_exp)*
- *UPPER(string_exp)*
- *IFNULL (expr, default_val)*
- *ISNULL (expr, default_val)*
- *NVL (expr, default_val)*
- *CONVERT (value_exp, data_type)*
- *CURDATE()*
- *CURTIME()*
- *CURTIMESTAMP()*
- *DATEADD(datepart, number, date)*
- *TIMESTAMPADD(datepart, number, date)*

- DATEDIFF(*datepart, startdate, enddate*) Para *datepart*, se permiten los valores de año, día y segundo.
- TIMESTAMPDIFF(*datepart, startdate, enddate*) Para *datepart*, se permiten los valores de año, día y segundo.
- DAYOFMONTH(*date_exp*)
- DAYOFWEEK(*date_exp*)
- DAYOFYEAR(*date_exp*)
- HOUR(*time_exp*)
- MINUTE(*time_exp*)
- MONTH(*date_exp*)
- NOW()
- SECOND(*time_exp*)
- WEEK(*date_exp*)
- YEAR(*date_exp*)
- AVG([ALL | DISTINCT]*expression*)
- SUM([ALL | DISTINCT]*expression*)
- COUNT([ALL | DISTINCT]*expression* | *)
- MAX([ALL | DISTINCT]*expression*)
- MIN([ALL | DISTINCT]*expression*)

Procesamiento de las consultas

CA Enterprise Log Manager procesa una consulta iniciada por el cliente de ODBC o JDBC del modo siguiente:

1. Una aplicación cliente envía una instrucción SELECT a través de una conexión ODBC con el servidor de CA Enterprise Log Manager.
2. El servidor de CA Enterprise Log Manager valida la instrucción SELECT. Si la validación es correcta, el servidor de CA Enterprise Log Manager crea una estructura de datos que representa la consulta.

Los errores detectados se envían directamente al controlador del cliente.

3. El servidor de CA Enterprise Log Manager convierte los elementos SQL en una consulta que puede emplear. Si la conversión es correcta, el servidor de CA Enterprise Log Manager ejecuta la consulta.
Los errores detectados se envían al controlador del cliente.
4. El servidor de CA Enterprise Log Manager gestiona la información sobre el estado de cada consulta, incluido un temporizador de caducidad, de manera que la consulta se pueda cancelar en caso de que la sesión se cierre o de que la consulta caduque.
5. El servidor de CA Enterprise Log Manager traduce los resultados de la consulta y los envía de vuelta al controlador del cliente de ODBC; a continuación, la aplicación cliente recibe los datos.

Alias de la columna de resultado

Como parte de esta gestión del estado de las consultas, CA Enterprise Log Manager ofrece soporte para nombres de columnas de resultados con alias. Por lo tanto, puede visualizar campos de la gramática de eventos comunes en los informes personalizados con sus propias etiquetas y encabezados.

Los alias persisten y se emplean para la asignación de datos adecuada cuando el servidor de CA Enterprise Log Manager transfiere un conjunto de resultados al controlador del cliente.

Límites de resultados

Para gestionar el espacio en disco, CA Enterprise Log Manager limita el número de filas de resultados. CA Enterprise Log Manager emplea un subconjunto de la palabra clave Transact-SQL TOP con un solo valor fijo. La variante porcentual de la palabra clave no es compatible.

El valor TOP predeterminado empleado en CA Enterprise Log Manager es de 5.000 filas, con un valor máximo de 50.000 filas.

Códigos de error específicos de CA Enterprise Log Manager

A continuación, se indican los códigos de error de ODBC y JDBC que pueden producirse al acceder al almacén de registro de eventos de CA Enterprise Log Manager. Cada mensaje de error ofrece detalles específicos del error.

- 88: error de compatibilidad
El mensaje de error que lo acompaña ofrece detalles sobre la funcionalidad no compatible.
- 300: error genérico
El mensaje de error que lo acompaña ofrece detalles.
- 301: error al convertir parámetros de caracteres de varios bytes
- 302: error de autenticación
- 304: expresión (columna) no válida en la cláusula OrderBy o GroupBy

Los errores siguientes son errores de ejecución de instrucciones SQL:

- 305: error al iniciar una consulta
- 306: error al obtener el estado de una consulta
- 307: error al analizar el XML de resultados de una consulta
- 308: error de ejecución de consulta
- 309: consulta ejecutada con errores
- 310: error al recuperar los resultados de una consulta
- 311: tiempo de espera de consulta transcurrido

Ejemplo: Empleo de un filtro de acceso para limitar los resultados de ODBC

Puede crear un filtro de acceso para limitar los datos obtenidos por una consulta de acceso de ODBC. Cuando miembros del grupo de aplicaciones mencionado acceden a datos de eventos de CA Enterprise Log Manager mediante el cliente de ODBC, sólo ven la información permitida por el filtro.

En este ejemplo, se presupone que tiene un grupo de aplicaciones llamado Analistas_UNIX y que quiere hacer que todos los miembros de ese grupo sólo vean los eventos de UNIX del almacén de registro de eventos. El filtro creado en este ejemplo limita la visualización de datos de eventos de la interfaz de usuario de CA Enterprise Log Manager y solicitudes externas mediante ODBC.

En la ayuda en línea, podrá obtener más información sobre filtros de acceso.

Para crear filtros de acceso

1. Inicie sesión en CA Enterprise Log Manager como Administrator.
2. Haga clic en la ficha Administración y, a continuación, en la subficha Gestión de usuarios y accesos.
3. Haga clic en Nuevo filtro de acceso . Se inicia el asistente de diseño de filtro de acceso.
4. Introduzca Analistas de UNIX en el campo de nombre, y la frase Filtro de acceso de analistas de UNIX en el campo de descripción. A continuación, haga clic en el paso 2 de identidades en la parte superior del cuadro de diálogo.
5. Cambie el tipo a Grupo de aplicaciones y escriba UNIX en el campo de nombre. A continuación, haga clic en Buscar identidades.

En un control de cambio, aparece una lista de identidades que coinciden con los criterios de búsqueda para que pueda seleccionar las identidades deseadas.
6. Seleccione el grupo de aplicaciones Analistas_UNIX en la lista Identidades disponibles y haga clic en el control de cambio de flecha hacia la derecha para desplazar la selección a la lista Identidades seleccionadas.
7. Haga clic en el paso 3 de filtros de acceso en la parte superior del cuadro de diálogo.
8. Haga clic en Nuevo filtro de evento  para agregar una línea y, a continuación, haga clic en el área de campo situada bajo Columna.
9. Seleccione event_logname en la lista desplegable y, a continuación, haga clic en el área de campo situada bajo Valor.

10. Seleccione Unix en la lista desplegable. El cuadro de diálogo tendrá un aspecto parecido a este:

Diseño del filtro de acceso

UNIX_Analysts

Guardar Guardar y cerrar Cancelar R

1 Detalles 2 Identities 3 Filtros de acceso

● = Requerido

Filtros avanzados

Para filtrar los eventos, defina una sentencia condicional en el control de filtros.

Lógica	Columna	Operador	Valor
	event_logname	Igual a	Unix

11. Haga clic en Guardar y cerrar.

Ejemplo: Preparación para el uso de clientes de ODBC y JDBC con Crystal Reports

La preparación para el acceso de clientes de ODBC o JDBC a eventos de CA Enterprise Log Manager mediante BusinessObjects Crystal Reports consta de los pasos siguientes:

1. Cree un usuario de CA Enterprise Log Manager para permitir un acceso a la base de datos.
2. Compruebe que el servicio ODBC emplea un cifrado SSL y el puerto 17002.
3. Instale el cliente de ODBC o copie los archivos de JDBC en el servidor en el que se encuentra Crystal Reports.

Consulte la *Guía de implementación* para obtener información sobre estas instalaciones.

4. Configure los componentes del sistema operativo:
 - a. Cree y pruebe un origen de datos de ODBC en el panel de control de Windows.
 - b. Edite el archivo de configuración de Crystal Reports para emplear el cliente de JDBC.

5. Cree eventos para su recopilación mediante CA Enterprise Log Manager.

Si está seguro de que el almacén de registro de eventos ya contiene eventos del tipo consultado, puede omitir este paso.

Nota: Este proceso y el ejemplo relacionado dan por hecho que está familiarizado con la creación de instrucciones SQL básicas y con el empleo de Crystal Reports. Puede obtener más información sobre el uso de Crystal Reports en la ayuda en línea de BusinessObjects.

Creación de un usuario de CA Enterprise Log Manager para el acceso de ODBC o JDBC

Utilice este proceso para crear una cuenta de usuario llamada ELM_Access para emplearla con los clientes de JDBC y ODBC.

Los usuarios de CA Enterprise Log Manager con permiso de acceso a datos pueden emplear ODBC o JDBC para acceder a datos de eventos. Cada uno de los roles de usuario predeterminados que se ofrecen en CA Enterprise Log Manager cuenta con este permiso. En el caso de este ejemplo, podría crear un usuario con cualquiera de los roles de CA Enterprise Log Manager predeterminados: Administrator, Analyst o Auditor.

Para crear un nuevo usuario

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario Administrator.
2. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
3. Haga clic en el botón Usuarios para mostrar la interfaz de usuario de CA EEM incrustada.
4. Haga clic en Nuevo usuario. Se abre el cuadro de diálogo Nuevo usuario.
5. Haga clic en Agregar detalles de usuario de aplicación y otorgue a la cuenta privilegios de aplicación de Administrator.

Nota: En un entorno de producción, asignaría el permiso mínimo necesario para que un usuario acceda a los datos. Puede limitar el acceso de diferentes formas, incluidos roles de usuario, políticas de acceso y filtros de acceso. Consulte la *Ayuda en línea* para obtener más información.

6. Complete el registro de usuario según proceda y asigne una contraseña, anotándola para su uso posterior en este ejemplo.
7. Guarde el usuario y cierre la ventana Usuarios.

Configuración de los ajustes de servicio ODBC

Utilice este procedimiento para configurar los ajustes de servicio ODBC y JDBC de CA Enterprise Log Manager.

Nota: Los cambios realizados en esta área provocan un reinicio de los procesos por parte del servidor que permite la comunicación de ODBC y JDBC.

Para configurar el servicio ODBC

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario Administrator.
2. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
3. Haga clic en el nodo de servicio ODBC.
4. Acepte la configuración predeterminada:
 - Activar servicio: Verdadero (permite la conexión de ODBC y JDBC en el servidor de CA Enterprise Log Manager)
 - Puerto: 17002
 - Cifrado (Capa de sockets seguros) está seleccionado
 - Tiempo de espera de sesión: 15 minutos
 - Nivel de registro: acepte el valor predeterminado, NO ESTABLECIDO
5. Haga clic en Guardar.

Creación de un origen de datos ODBC "elm"

Utilice este procedimiento para crear un origen de datos llamado "CA-ELM."

Nota: Instale el cliente de ODBC antes de configurar el origen de datos.

Para crear orígenes de datos

1. Abra el Panel de control de Windows.
2. Abra la carpeta Herramientas administrativas e inicie la utilidad Orígenes de datos (ODBC).
3. Haga clic en Agregar para mostrar el cuadro de diálogo Crear nuevo origen de datos.

4. Seleccione la entrada, DataDirect OpenAccess SDK 6.0 y haga clic en Finalizar.

La utilidad DataDirect OpenAccess SDK ODBC Driver Setup muestra una pantalla de configuración.

5. Introduzca CA-ELM en el campo de nombre de origen de datos y ofrezca una descripción textual.
6. Introduzca el nombre del servidor de CA Enterprise Log Manager en el campo de host de servicio. En este ejemplo, se emplea ca-elm.
7. Introduzca 17002 en el campo de puerto de servicio.
8. Seleccione la casilla de verificación Cifrado (Capa de sockets seguros).
9. Introduzca las propiedades personalizadas siguientes:

```
querytimeout=600  
(seconds);queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false
```

10. Haga clic en Aplicar y, a continuación, en Probar conexión.

Si los parámetros de conexión son correctos, aparece un mensaje de conexión correcta.

11. Haga clic en Aceptar para volver al cuadro de diálogo de administrador de origen de datos de ODBC y vuelva a hacer clic en Aceptar para cerrar la utilidad.

Consideraciones de origen de datos de ODBC

A continuación, se indican descripciones de los campos de origen de datos de ODBC según su relación con CA Enterprise Log Manager:

Nombre de origen de datos

Cree un nombre para este origen de datos. Las aplicaciones cliente que desean emplear este dato utilizan este nombre para conectarse al origen de datos.

Host de servicio

Indica el nombre del servidor de CA Enterprise Log Manager al que se conecta el cliente. Puede emplear un nombre de host o una dirección IPv4.

Puerto de servicio

Especifica el puerto de servicio de TCP en el que el servidor de CA Enterprise Log Manager escucha las conexiones de clientes de ODBC. El valor predeterminado es 17002. El valor definido aquí debe coincidir con la configuración del servicio del servidor de ODBC; si no es así, la conexión no será correcta.

Origen de datos de servicio

Deje este campo en blanco; si no lo hace, el intento de conexión fallará.

Cifrado SSL

Especifica si se debe emplear cifrado en las comunicación entre el cliente y el servidor de CA Enterprise Log Manager. El valor predeterminado es tener SSL activado. El valor definido aquí debe coincidir con la configuración del servicio del servidor de ODBC; si no es así, la conexión no será correcta.

Propiedades personalizadas

Indica las propiedades de conexión para su empleo con el almacén de registro de eventos. El delimitador de las propiedades es un punto y coma sin espacio. Los valores predeterminados recomendados incluyen los siguientes:

querytimeout

Indica el valor del tiempo de espera en segundos sin obtención de datos tras el que se cierra la consulta. A continuación, se muestra la sintaxis de esta propiedad:

```
querytimeout=300
```

queryfederated

Indica si se va a realizar una consulta federada. El establecimiento de este valor como falso sólo realiza una consulta en el servidor de CA Enterprise Log Manager en el que se realiza la conexión de la base de datos. A continuación, se muestra la sintaxis de esta propiedad:

```
queryfederated=true
```

queryfetchrows

Define la cantidad de filas que se deben recuperar en una sola operación de recuperación si la consulta es correcta. El valor mínimo es 1 y el máximo, 5000. El valor predeterminado es 1000. A continuación, se muestra la sintaxis de esta propiedad:

```
queryfetchrows=1000
```

offsetmins

Especifica la diferencia de zona horaria del cliente de ODBC. El valor 0 aplica GMT. Puede emplear este campo para definir su propia diferencia de zona horaria con respecto a GMT. A continuación, se muestra la sintaxis de esta propiedad:

```
offsetmins=0
```

suppressNoncriticalErrors

Indica el comportamiento del proveedor de la interfaz en el caso de errores no críticos como que una base de datos no responda o que un host no responda.

A continuación, se muestra la sintaxis de esta propiedad:

```
suppressNoncriticalErrors=false
```

Edición del archivo de configuración de Crystal Reports

Antes de poder emplear Crystal Reports con el cliente de JDBC de CA Enterprise Log Manager, debe realizar algunos ajustes de configuración. Después de configurar el archivo de configuración XML de Crystal Reports, estará listo para preparar y enviar consultas estándar de ANSI SQL al almacén de registro de eventos de CA Enterprise Log Manager.

Para configurar los ajustes de Crystal Reports para JDBC

1. Asegúrese de que copia los archivos JAR del cliente de JDBC en el servidor de Crystal Reports antes de editar el archivo de configuración.

Si desea más información, puede consultar la *Guía de implementación*.

2. Acceda al servidor en el que se encuentra Crystal Reports.
3. Localice el archivo, CRConfig.xml, y ábralo para editarlo.

4. Localice la etiqueta <DataDriverCommon> y la sección de la etiqueta <Classpath> situada bajo ella.
5. Agregue la ubicación de los archivos JAR de JDBC para el cliente de JDBC a classpath.

6. Cambie el valor de las etiquetas URL de JDBC por lo siguiente:

```
jdbc:ca-elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

Consulte la sección sobre consideraciones de URL de JDBC para obtener más explicaciones sobre estos parámetros.

Consulte la documentación proporcionada con Crystal Reports para obtener más información acerca de la configuración de los parámetros de conexión de dicho producto.

7. Cambie el valor de las etiquetas Classname de JDBC por lo siguiente:

```
com.ca.jdbc.openaccess.OpenAccessDriver
```

8. Guarde el archivo y cierre.

Más información:

[Consideraciones de URL de JDBC](#) (en la página 718)

Consideraciones de URL de JDBC

Al emplear el cliente de JDBC para acceder a los datos de eventos almacenados en CA Enterprise Log Manager, necesita tanto Classpath de JDBC como URL de JDBC. Classpath de JDBC indica las ubicaciones de los archivos JAR del controlador. URL de JDBC define los parámetros que emplean las clases de los archivos JAR al cargarse.

A continuación, se indica un ejemplo completo de URL de JDBC:

```
jdbc:ca-elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

Las descripciones siguientes definen los componentes de URL:

`jdbc.ca-elm:`

Define la cadena protocol:subprotocol que designa el controlador de JDBC suministrado con CA Enterprise Log Manager.

//IP Address:Port;

Indica la dirección IP que representa al servidor de CA Enterprise Log Manager a cuyos datos desea acceder. El número de puerto es el puerto que se empleará para las comunicaciones y debe coincidir con los ajustes del panel de configuración del servicio ODBC de CA Enterprise Log Manager. Si los puertos no coinciden, el intento de conexión no es correcto.

encrypted=0|1;

Determina si el cifrado SSL se emplea para la comunicación entre el cliente de JDBC y el servidor de CA Enterprise Log Manager. El valor predeterminado es 0, sin cifrado, y no requiere una especificación en la URL. Setting encrypted=1 activa el cifrado. Defina la conexión del cifrado de forma explícita. Además, este ajuste debe coincidir con la configuración del cuadro de diálogo de servicio ODBC de CA Enterprise Log Manager. Si no es así, el intento de conexión no será correcto.

ServerDataSource=Default

Especifica el nombre del origen de los datos. Establezca este valor en *Predeterminado* para acceder al almacén de registro de eventos de CA Enterprise Log Manager.

CustomProperties={x;y;z}

Estas propiedades son las mismas que las propiedades personalizadas de ODBC. Si no las especifica de forma explícita, se aplican los valores predeterminados en la URL de ejemplo.

Más información

[Consideraciones de origen de datos de ODBC](#) (en la página 715)

Creación de eventos para el ejemplo de ODBC

Para mostrar la consulta de muestra, cree algunos eventos relevantes ocasionando actividades erróneas como las siguientes:

- Inicie sesión de forma incorrecta en el servidor de CA Enterprise Log Manager varias veces.
- Inicie sesión de forma incorrecta en un host de agente cuyos eventos vayan a un servidor de CA Enterprise Log Manager determinado.
- Acceda a un recurso de sistema o de red con credenciales incorrectas.

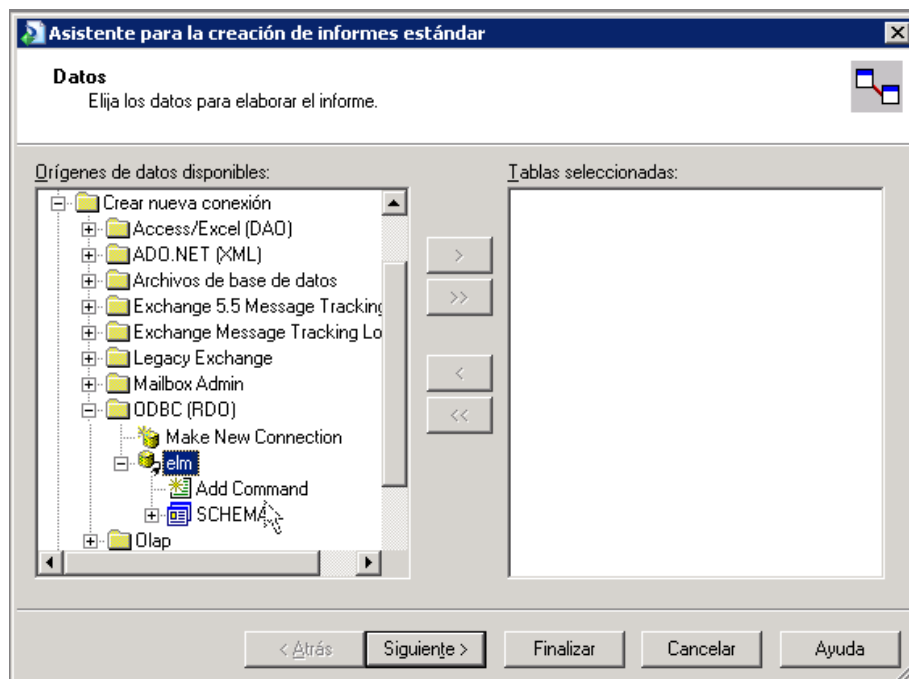
Uso de Crystal Reports para acceder al almacén de registro de eventos con ODBC

Puede emplear la funcionalidad de acceso de ODBC para realizar consultas sobre datos de eventos de CA Enterprise Log Manager desde una herramienta de realización de informes de terceros como BusinessObjects Crystal Reports. Después de realizar la instalación y las configuraciones necesarias, estará listo para preparar y enviar consultas estándar de ANSI SQL al almacén de registro de eventos de CA Enterprise Log Manager.

El esquema de la base de datos del almacén de registro de eventos es la gramática de eventos comunes. La ayuda en línea de CA Enterprise Log Manager contiene un componente de referencia de la gramática de eventos comunes para ayudarle a crear consultas. También puede revisar las instrucciones de SQL subyacentes para las consultas predeterminadas, pero debe emplear ANSI SQL para acceder a la base de datos desde fuera de CA Enterprise Log Manager.

Para acceder a datos de eventos desde Crystal Reports

1. Lleve a cabo las tareas de requisitos previos de instalación y configuración.
2. Inicie Crystal Reports y acceda al asistente de informes estándar.
3. Cree una conexión de ODBC en el cuadro de diálogo de datos y seleccione el origen de datos de ODBC creado en el Panel de control de Windows.



4. Utilice la funcionalidad de adición de comandos para crear una consulta en el área de introducción de SQL.

Por ejemplo, es posible crear la consulta siguiente:

```
SELECT source_username as source_username , SUM(event_count) AS  
FUNC_SUM_event_count FROM view_event WHERE event_result = 'F' GROUP BY  
source_username ORDER BY FUNC_SUM_event_count DESC;
```

5. Haga clic en Aceptar para finalizar la introducción de la consulta.

Aparece una plantilla de informe en la que hay que colocar las columnas de datos obtenidas por la consulta.

6. Arrastre y suelte los campos del explorador de campos de la esquina superior derecha en la plantilla de informes como columnas.

La ejecución de la consulta muestra los valores asociados a los campos. Puede emplear Crystal Reports para crear cualquier visualización o personalización que necesite.

7. (Opcional) Compare los resultados del informe con el informe predeterminado, "Actividad errónea por ejecutor".

Acceso a eventos desde Crystal Reports con JDBC

Las tareas siguientes le permiten emplear JDBC para acceder al almacén de registro de eventos:

1. Copie los archivos JDBC JAR del cliente en el servidor en el que se encuentra Crystal Reports.
2. Edite el archivo de configuración de Crystal Reports.
3. Utilice Crystal Reports para enviar una consulta.

Nota: Este proceso y el ejemplo relacionado dan por hecho que está familiarizado con la creación de instrucciones SQL básicas y con el empleo de Crystal Reports. Puede obtener más información sobre el uso de Crystal Reports en la ayuda en línea de BusinessObjects.

Copia de archivos JAR del controlador de JDBC

Antes de utilizar el controlador de JDBC para acceder a eventos de un servidor de CA Enterprise Log Manager, copie los archivos JAR relacionados en el servidor que desea emplear para el acceso.

Para copiar los archivos

1. Abra la imagen ISO o acceda al DVD de instalación de la aplicación.
2. Desplácese al directorio \CA\ELM\JDBC.
3. Copie los archivos JAR en el servidor en el que se encuentra Crystal Reports.
El paquete de informes que emplea requiere una ubicación específica para estos archivos. Consulte la documentación que se ofrece con la aplicación.
4. Anote el directorio en el que coloca estos archivos como ruta de referencia al configurar conexiones.

Uso de Crystal Reports para acceder al almacén de registro de eventos con JDBC

Puede emplear la funcionalidad de acceso de JDBC para realizar consultas sobre datos de eventos de CA Enterprise Log Manager de una herramienta de realización de informes de terceros como BusinessObjects Crystal Reports.

El esquema de la base de datos del almacén de registro de eventos es la gramática de eventos comunes. La ayuda en línea de CA Enterprise Log Manager contiene un componente de referencia de la gramática de eventos comunes para ayudarle a crear consultas. También puede revisar las instrucciones de SQL subyacentes para las consultas predeterminadas, pero debe emplear ANSI SQL para acceder a la base de datos desde fuera de CA Enterprise Log Manager.

Para acceder a datos de eventos desde Crystal Reports

1. Inicie Crystal Reports y acceda al asistente de informes estándar.
2. Cree una conexión JDBC en el cuadro de diálogo de datos.
Nota: Utilice el valor *Predeterminado* para Nombre de base de datos en el cuadro de diálogo Información de conexión cuando aparezca.
3. Utilice la funcionalidad de adición de comandos para crear y ejecutar la consulta siguiente en el área de introducción de SQL:

```
SELECT source_username as source_username , SUM(event_count) AS  
FUNC_SUM_event_count FROM view_event WHERE event_result = 'F' GROUP BY  
source_username ORDER BY FUNC_SUM_event_count DESC;
```

4. Arrastre y suelte los campos del explorador de campos de la derecha en la plantilla de informes como columnas.

La ejecución de la consulta muestra los valores asociados a los campos. Puede emplear las herramientas de Crystal Reports para crear cualquier visualización o personalización que necesite.

5. (Opcional) Compare los resultados del informe con el informe predeterminado, "Actividad errónea por ejecutor".

Supresión del cliente de ODBC en sistemas Windows

En todas las plataformas de Windows, la opción de eliminación del paquete de instalación del cliente borra los archivos y las entradas del producto de la información del sistema.

Importante: Si ha creado archivos de origen de IP en el directorio de instalación de cliente de ODBC local, realice una copia de seguridad de los archivos en una ubicación distinta antes de eliminar el cliente de ODBC de un sistema Windows.

Si tiene instalado el cliente de ODBC local y desea instalarlo en una ubicación diferente, utilice la opción de eliminación. Elimine el cliente de ODBC local instalado y, a continuación, vuelva a instalarlo en la ubicación nueva.

Para eliminar el cliente de ODBC

1. Abra la utilidad Agregar o quitar programas en el Panel de control de Windows.
2. Localice y seleccione la entrada, CA Enterprise Log Manager ODBC Driver.
3. Haga clic en Quitar.

Supresión de clientes de JDBC

Para desinstalar el cliente de JDBC, elimine el directorio de instalación.

Glosario

acceso a datos

El *acceso a datos* es un tipo de autorización que se ofrece a todos los servidores de CA Enterprise Log Manager mediante la política de acceso a datos predeterminada del tipo de recurso de CALM. Los usuarios pueden acceder a todos los datos, excepto a aquellos restringidos por filtros de acceso a datos.

Acceso de ODBC y JDBC

El *acceso de ODBC y JDBC* a los almacenes de registro de eventos de CA Enterprise Log Manager admite el empleo de datos de eventos con diversos productos de terceros, incluida la generación de informes de eventos mediante herramientas de generación de informes de terceros, la correlación de eventos mediante motores de correlación y la evaluación de eventos mediante productos de detección de intrusiones o software maligno. Los equipos con sistemas operativos Windows emplean el acceso de ODBC; los equipos con sistemas operativos UNIX y Linux emplean en acceso de JDBC.

actualizaciones de contenido

Las *actualizaciones de contenido* son la parte no binaria de las actualizaciones de suscripción que se almacenan en el servidor de gestión de CA Enterprise Log Manager. Las actualizaciones de contenido incluyen contenido como archivos XMP, archivos de asignación de datos, actualizaciones de configuración para módulos de CA Enterprise Log Manager y actualizaciones de claves públicas.

actualizaciones de suscripción

Las *actualizaciones de suscripción* hacen referencia a archivos binarios y no binarios que están disponibles mediante el servidor de suscripción de CA. Los archivos binarios son actualizaciones de módulos de productos que se suelen instalar en CA Enterprise Log Manager. Los archivos no binarios, o actualizaciones de contenido, se guardan en el servidor de gestión.

acumulación de eventos

La *acumulación de eventos* es el proceso a través del cual las entradas de registro similares se consolidan en una única entrada que contiene un recuento del número de repeticiones del evento. Las reglas de resumen definen cómo se acumulan los eventos.

adaptadores de CA

Los *adaptadores de CA* son un grupo de escuchas que reciben eventos de componentes de CA Audit como clientes de CA Audit, iRecorders y SAPI recorders, así como orígenes que envían eventos de forma nativa en iTechnology.

agente

Un *agente* es un servicio genérico configurado mediante conectores, cada uno de los cuales recopila eventos sin formato de un único origen de eventos y, a continuación, los envía a CA Enterprise Log Manager para procesarlos. Cada CA Enterprise Log Manager cuenta con un agente incorporado. Además, puede instalar un agente en un punto de recopilación remoto y, de este modo, recopilar eventos en host en los que no se pueden instalar agentes. Puede instalar un agente en el host en el que se ejecutan los orígenes de eventos y aprovechar las ventajas de la posibilidad de aplicar reglas de supresión y cifrar la transmisión a CA Enterprise Log Manager.

agente predeterminado

El *agente predeterminado* es el agente integrado que se instala con el servidor de CA Enterprise Log Manager. Puede configurarse para la recopilación directa de eventos de syslog, así como de eventos de diversos orígenes de eventos que no son de syslog, como CA Access Control r12 SP1, el servicio de certificados de Microsoft Active Directory y las bases de datos de Oracle9i.

alerta de acción

Una *alerta de acción* es una tarea de consulta programada que se puede emplear para detectar infracciones de políticas, tendencias de uso, patrones de inicio de sesión y otras acciones que pueden requerir atención a corto plazo. De forma predeterminada, cuando las consultas de alerta devuelven resultados, éstos se muestran en la página de alertas de CA Enterprise Log Manager y también se añaden a una fuente RSS. Al programar una alerta, puede especificar más destinos, incluido el correo electrónico, un proceso de obtención de resultados de eventos/alertas de CA IT PAM y traps de SNMP.

almacén de usuarios

Un *almacén de usuarios* es el repositorio de las políticas de contraseña y la información de usuario global. El almacén de usuarios de CA Enterprise Log Manager es el repositorio local predeterminado, pero se puede configurar para hacer referencia a CA SiteMinder o a un directorio de LDAP compatible como Microsoft Active Directory, Sun One o Novell eDirectory. Independientemente de cómo se configure el almacén de usuarios, el repositorio local del servidor de gestión contiene información específica de la aplicación sobre usuarios, como su función y las políticas de acceso asociadas.

almacenamiento automático

El *almacenamiento automático* es un proceso configurable que automatiza el desplazamiento de bases de datos de archivo de un servidor a otro. En la primera fase del almacenamiento automático, el servidor de recopilación envía las bases de datos recién almacenadas al servidor de informes con la frecuencia establecida. En la segunda fase, el servidor de informes envía las bases de datos antiguas al servidor de almacenamiento remoto para su almacenamiento a largo plazo, evitando así la necesidad de realizar una copia de seguridad manual y un desplazamiento. El almacenamiento automático requiere que configure una autenticación sin contraseña del origen al servidor de destino.

almacenamiento de registro de eventos

El *almacenamiento de registro de eventos* es el resultado del proceso de almacenamiento, durante el que el usuario realiza una copia de seguridad de una base de datos tibia, notifica a CA Enterprise Log Manager mediante la ejecución de la utilidad LMArchive y desplaza la base de datos con copia de seguridad del almacenamiento de registro de eventos al almacenamiento a largo plazo.

almacenamiento de registro de eventos

El *almacenamiento de registro de eventos* es un componente del servidor de CA Enterprise Log Manager en el que los eventos entrantes se almacenan en bases de datos. Las bases de datos del sistema de almacenamiento de registro de eventos deben tener copias de seguridad hechas a mano y se deben trasladar a una ubicación de almacenamiento de registros remota antes de la fecha configurada para su eliminación. Las bases de datos almacenadas se pueden restaurar en un sistema de almacenamiento de registro de eventos.

almacenamiento de registros

El *almacenamiento de registros* es el proceso de lo que sucede cuando la base de datos caliente alcanza el tamaño máximo, momento en que se lleva a cabo la compresión de las filas y el estado pasa de caliente a tibio. Los administradores deben realizar copias de seguridad manuales de las bases de datos tibias antes de que se alcance el umbral de eliminación. También deben ejecutar la utilidad LMArchive para registrar el nombre de las copias de seguridad. Esta información se puede visualizar a través de la consulta de archivos.

análisis

El *análisis*, también denominado análisis de mensajes (MP), es el proceso de conversión de datos sin formato del dispositivo en pares clave-valor. El análisis se lleva a cabo mediante un archivo XMP. El análisis, que precede a la asignación de datos, es un paso del proceso de integración que convierte el evento sin formato recopilado de un origen de eventos en un evento refinado que se puede visualizar.

análisis de archivos XMP

El *análisis de archivos XMP* es el proceso que lleva a cabo la utilidad de análisis de mensajes para buscar todos los eventos que contienen cada una de las cadenas de coincidencia previa y, para cada evento coincidente, analizar el evento en tokens mediante el primer filtro detectado que emplee la misma cadena de coincidencia previa.

análisis de asignaciones

El *análisis de asignaciones* es un paso del asistente para el archivo de asignación que le permite comprobar y realizar cambios en un archivo de asignación de datos (DM). Los eventos de ejemplo se prueban con respecto al archivo de asignación de datos y los resultados se validan con la gramática de eventos comunes.

análisis de mensajes

El *análisis de mensajes* es el proceso de aplicación de reglas al análisis de un registro de eventos sin formato para obtener información relevante como la indicación de tiempo, la dirección IP y el nombre de usuario. Las reglas de análisis emplean la coincidencia de caracteres para ubicar determinado texto de eventos y vincularlo a los valores seleccionados.

análisis de registros

El *análisis de registros* es el estudio de las entradas de registro para identificar los eventos de interés. Si los registros no se analizan de forma periódica, su valor se reduce en gran medida.

análisis de registros

El *análisis de registros* es el proceso de extracción de datos de un registro de manera que los valores analizados se pueden emplear en una etapa posterior de la gestión de registros.

archivo de análisis de mensajes (XMP)

Un *archivo de análisis de mensajes (XMP)* es un archivo XML asociado a un tipo de origen de evento específico que aplica reglas de análisis. Las reglas de análisis dividen los datos relevantes de un evento sin formato recopilado en pares nombre-valor que se transfieren al archivo de asignación para continuar el procesamiento. Este tipo de archivo se emplea en todas las integraciones y en los conectores que se basan en integraciones. En el caso de los adaptadores de CA, los archivos XMP también se pueden aplicar en el servidor de CA Enterprise Log Manager.

archivos de asignación de datos (DM)

Los *archivos de asignación de datos (DM)* son archivos XML que emplean la gramática de eventos comunes (CEG) de CA para transformar eventos del formato de origen a un formato compatible con la gramática de eventos comunes con el fin de poder almacenarlos para realizar informes y análisis en el sistema de almacenamiento de registro de eventos. Es necesario crear un archivo de asignación de datos para cada nombre de registro para poder almacenar datos de eventos. Los usuarios pueden modificar o copiar un archivo de asignación de datos y aplicarlo a un determinado conector.

asignación de datos (DM)

La *asignación de datos* es el proceso de asignación de los pares clave-valor en la gramática de eventos comunes. La asignación de datos se lleva a cabo mediante un archivo de asignación de datos.

asignaciones de función

Las *asignaciones de función* son una parte opcional del archivo de asignación de datos para una integración del producto. Las asignaciones de funciones se emplean para rellenar un campo de la gramática de eventos comunes cuando el valor requerido no se puede obtener directamente del evento de origen. Todas las asignaciones de función constan de un nombre de campo de gramática de eventos comunes, un valor de campo predefinido o de clase y la función empleada para obtener o calcular el valor.

asistente para el archivo de análisis

El *asistente para el archivo de análisis* es una función de CA Enterprise Log Manager que emplean los administradores para crear, editar y analizar archivos eXtensible Message Parsing (XMP) almacenados en el servidor de gestión de CA Enterprise Log Manager. La personalización del análisis de los datos de eventos entrantes incluye la edición de filtros y cadenas de coincidencias previas. Los archivos nuevos y los editados se muestran en el explorador de recopilaciones, en la biblioteca de refinamiento de eventos, en los archivos de análisis de la carpeta de usuarios.

autenticación ssh no interactiva

La autenticación *no interactiva* permite que los archivos se desplacen de un servidor a otro sin tener que introducir una frase de contraseña para la autenticación. Configure la autenticación no interactiva del servidor de origen al servidor de destino antes de configurar el archivado automático o utilizar el script `restore-ca-elm.sh`.

base de datos en estado tibio

El *estado tibio de una base de datos* es el estado en el que se encuentra una base de datos de registros de eventos cuando se supera el tamaño (Número máximo de filas) de la base de datos caliente o cuando se lleva a cabo una recatalogación tras restaurar una base de datos fría en un sistema de almacenamiento de registro de eventos nuevo. Las bases de datos tibias se comprimen y se retienen en el sistema de almacenamiento de eventos hasta que su antigüedad en días supera el valor configurado para Número máximo de días de archivado. Puede realizar consultas en registros de eventos de bases de datos en estado caliente, tibio y descongelado.

bases de datos archivadas

Las *bases de datos archivadas* de un determinado servidor de CA Enterprise Log Manager incluyen todas las bases de datos tibias que están disponibles para realizar consultas pero que deben poseer copias de seguridad antes de caducar, todas las bases de datos frías que se han registrado como poseedoras de copias de seguridad, así como todas las bases de datos registradas como restauradas a partir de copias de seguridad.

biblioteca de análisis de mensajes

La *biblioteca de análisis de mensajes* es una biblioteca que acepta eventos de las colas de escucha y emplea expresiones regulares para convertir las cadenas de pares nombre/valor mediante tokens.

biblioteca de consultas

La *biblioteca de consultas* es la biblioteca que almacena todas las consultas predefinidas y definidas por el usuario, las etiquetas de consultas y los filtros de solicitudes.

biblioteca de informes

La *biblioteca de informes* es la biblioteca que almacena todos los informes predefinidos y definidos por el usuario, las etiquetas de informes y las tareas de informes programadas.

biblioteca de refinamiento de eventos

La *biblioteca de refinamiento de eventos* es el sistema de almacenamiento de integraciones predefinidas y definidas por el usuario, archivos de asignación y análisis, así como reglas de supresión y resumen.

CA Enterprise Log Manager

CA Enterprise Log Manager es una solución que le ayuda a recopilar registros de diversos tipos de orígenes de eventos dispersos, comprobar la conformidad con las consultas y los informes, así como guardar entradas de bases de datos de registros comprimidos que ha trasladado a sistemas de almacenamiento externos a largo plazo.

CA IT PAM

CA IT PAM es la forma abreviada de CA IT Process Automation Manager. Este producto de CA automatiza los productos que haya definido.

CA Enterprise Log Manager emplea dos procesos: el proceso de creación de un proceso de obtención de eventos/alertas para un producto local, como CA Service Desk; y el proceso de generación dinámica de listas que pueden importarse como valores con clave. La integración requiere CA IT PAM r2.1.

CA Spectrum

CA Spectrum es un producto de gestión de errores de red que se puede integrar con CA Enterprise Log Manager para emplearlo como destino de las alertas enviadas en forma de traps de SNMP.

CAELM

CAELM es el nombre de la instancia de la aplicación que emplea CA EEM para CA Enterprise Log Manager. Para acceder a la funcionalidad de CA Enterprise Log Manager en CA Embedded Entitlements Manager, introduzca la URL: https://<ip_address>:5250/spin/eiam/eiam.csp, seleccione CAELM como nombre de la aplicación e introduzca la contraseña del usuario de EiamAdmin.

caelmadmin

El nombre de usuario y la contraseña de *caelmadmin* son las credenciales necesarias para acceder al sistema operativo del dispositivo de software. El ID de usuario de caelmadmin se crea durante la instalación de este sistema operativo. Durante la instalación del componente de software, el instalador debe especificar la contraseña de la cuenta del superusuario de CA EEM, EiamAdmin. La cuenta de caelmadmin tendrá la misma contraseña. Es recomendable que el administrador del servidor realice ssh como usuario de caelmadmin y cambie esta contraseña predeterminada. Aunque el administrador no puede realizar ssh como raíz, sí puede trasladar a los usuarios a la raíz (su root) si lo considera necesario.

caelmservice

caelmservice es una cuenta de servicio que permite a iGateway y a los servicios de CA EEM locales ejecutarse como un usuario no-root. La cuenta caelmservice se emplea para instalar actualizaciones del sistema operativo descargadas con actualizaciones de suscripción.

calendario

Un *calendario* es un sistema para limitar las veces que una política de acceso es efectiva. Una política permite que determinadas identidades lleven a cabo acciones especificadas con respecto a cierto recurso durante un tiempo determinado.

CALM

CALM es un tipo de recurso predefinido que incluye los recursos de CA Enterprise Log Manager siguientes: Alert, ArchiveQuery, calmTag, Data, EventGrouping, Integration y Report. Las acciones permitidas en este tipo de recurso son Anotar (Reports), Crear (Alert, calmTag, EventGrouping, Integration y Report), Acceso a datos (Data), Ejecutar (ArchiveQuery) y Programar (Alert, Report).

calmTag

calmTag es un atributo de Objeto aplicación que se emplea al crear políticas de ámbito para limitar a los usuarios a los informes y las consultas pertenecientes a determinadas etiquetas. Todos los informes y las consultas son Objetos aplicación y tienen calmTag como atributo. (Esto no debe confundirse con la etiqueta de recursos.)

Campos de la gramática de eventos comunes

Los *campos de la gramática de eventos comunes* son etiquetas empleadas para estandarizar la presentación de campos de eventos sin formato de diversos orígenes de eventos. Durante el refinamiento de eventos, CA Enterprise Log Manager analiza mensajes de eventos en una serie de pares de nombres y valores y, a continuación, asigna los nombres de eventos sin formato a campos de la gramática de eventos comunes estándar. Este refinamiento crea pares de nombres y valores que constan de campos de la gramática de eventos comunes y de valores del evento sin formato. Esto quiere decir que las diferentes etiquetas empleadas en eventos sin formato para el mismo objeto de datos o elemento de red se convierten con el mismo nombre de campo de la gramática de eventos comunes al refinar los eventos sin formato. Los campos de la gramática de eventos comunes se asignan al OID en la MIB empleada para traps de SNMP.

carpeta

Una *carpeta* es la ubicación de la ruta del directorio que emplea el servidor de gestión de CA Enterprise Log Manager para almacenar los tipos de objetos de CA Enterprise Log Manager. Se hace referencia a carpetas en las políticas de ámbito para otorgar o denegar a los usuarios el derecho a acceder a un tipo de objeto determinado.

catálogo

El *catálogo* es la base de datos de cada CA Enterprise Log Manager que mantiene el estado de las bases de datos guardadas, al tiempo que actúa como un índice de alto nivel en todas las bases de datos. La información sobre el estado (caliente, tibio o descongelado) se mantiene para todas las bases de datos presentes en algún momento en este servidor de CA Enterprise Log Manager y para cualquier base de datos que se haya restaurado en este servidor de CA Enterprise Log Manager como base de datos descongelada. La capacidad de indexación se extiende a todas las bases de datos calientes y tibias del sistema de almacenamiento de eventos de este servidor de CA Enterprise Log Manager.

catálogo de archivos

Consulte catálogo.

categorías de eventos

Las *categorías de eventos* son etiquetas empleadas por CA Enterprise Log Manager para clasificar eventos por su función antes de insertarlos en el almacén de eventos.

certificados

Los *certificados* que CA Enterprise Log Manager utiliza de modo predeterminado son CAELMCert.cer y CAELM_AgentCert.cer. Todos los servicios CA Enterprise Log Manager utilizan CAELMCert.cer para comunicar con el servidor de gestión. Todos los agentes utilizan CAELM_AgentCert.cer para comunicar con su servidor de recopilación.

cliente de suscripción

Un *cliente de suscripción* es un servidor de CA Enterprise Log Manager que obtiene contenido de otro servidor de CA Enterprise Log Manager denominado servidor proxy de suscripción. Los clientes de suscripción sondean el servidor proxy de suscripción configurado de manera regular y recuperan las actualizaciones nuevas cuando están disponibles. Tras recuperar las actualizaciones, el cliente instala los componentes descargados.

compatible con FIPS 140-2

Compatible con FIPS 140-2 es una designación para un producto que puede, *de forma opcional*, utilizar las bibliotecas y algoritmos criptográficos que cumplen con FIPS que se emplean para cifrar y descifrar datos confidenciales. CA Enterprise Log Manager es un producto de recopilación de registros compatible con FIPS debido a que se puede seleccionar si se desea ejecutar el programa en modo FIPS o en modo no FIPS.

complemento de eventos iTech

El *complemento de eventos iTech* es un adaptador de CA que puede configurar un administrador con archivos de asignación seleccionados. Recibe eventos de forma remota de iRecorders, CA EEM, la propia iTechnology o cualquier producto que envía eventos mediante iTechnology.

componentes de visualización

Los *componentes de visualización* son opciones disponibles para mostrar datos de informes que incluyen una tabla, un gráfico (gráfico de escala, gráfico de barras, gráfico de columnas, gráfico circular) o un visor de eventos.

conector

Un *conector* es la integración de un determinado origen de evento que se configura en un agente determinado. Un agente puede cargar múltiples conectores de tipos similares o distintos en la memoria. El conector permite la recopilación de eventos sin formato de un origen de eventos, así como la transmisión basada en reglas de los eventos convertidos a un sistema de almacenamiento de registro de eventos, donde se introducen en la base de datos caliente. Las integraciones predeterminadas permiten realizar una recopilación optimizada de un amplio rango de orígenes de eventos, incluidos sistemas operativos, bases de datos, servidores Web, cortafuegos y muchos tipos de aplicaciones de seguridad. Puede definir un conector para un origen de evento propio desde el principio o puede emplear para ello una integración a modo de plantilla.

configuración global

La *configuración global* es una serie de ajustes que se aplica a todos los servidores de CA Enterprise Log Manager que emplean el mismo servidor de gestión.

configuración guardada

Una *configuración guardada* es una configuración almacenada con los valores de los atributos de acceso a los datos de una integración que se puede emplear como plantilla al crear una integración nueva.

consulta

Una *consulta* es un conjunto de criterios empleado para realizar búsquedas en los sistemas de almacenamiento de registro de eventos del servidor de CA Enterprise Log Manager activo y, si se especifica, de sus servidores federados. Una consulta se dirige a las bases de datos calientes, tibias o descongeladas especificadas en la cláusula de la consulta. Por ejemplo, si la cláusula *Dónde* limita la consulta a eventos con el origen `source_username="myname"` en un determinado intervalo de tiempo y sólo 10 de las 1.000 bases de datos contienen registros que cumplen los criterios basados en información contenida en la base de datos del catálogo, la consulta sólo se ejecutará en esas 10 bases de datos. Una consulta sólo puede devolver un máximo de 5.000 filas de datos. Cualquier usuario con una función predefinida puede ejecutar una consulta. Sólo los analistas y los administradores pueden programar una consulta para distribuir una alerta de acción, crear un informe mediante la selección de las consultas que se van a incluir o crear una consulta personalizada mediante el asistente de diseño de consulta. Consulte también *consulta de archivo*.

consulta de acción

Una *consulta de acción* es una consulta que admite una alerta de acción. Se ejecuta en una programación repetitiva para probar las condiciones indicadas por la alerta de acción a la que está vinculada.

consulta de archivos

Una *consulta de archivos* es una consulta del catálogo que se emplea para identificar las bases de datos frías que se deben restaurar y descongelar para realizar consultas. Una consulta de archivos se diferencia de una consulta normal en que se realiza en bases de datos frías, mientras que una consulta normal se realiza en bases de datos calientes, tibias y descongeladas. Los administradores pueden emitir una consulta de archivos desde la ficha *Administración*, subficha *Recopilación de registros*, opción *Consulta de catálogo de archivos*.

Contenido de los trap de SNMP

Un *trap de SNMP* consta de pares de nombres y valores, donde cada nombre es un OID (identificador de objeto) y cada valor se obtiene de la alerta programada. Los resultados de consultas obtenidos por una alerta de acción constan de campos de la gramática de eventos comunes y sus valores. El trap de SNMP se rellena sustituyendo un OID para cada campo de la gramática de eventos comunes empleado para el nombre del par de nombre y valor. La asignación de cada campo de la gramática de eventos comunes a un OID se almacena en la MIB. El trap de SNMP sólo incluye pares de nombres y valores para los campos seleccionados al configurar la alerta.

cuenta

Una *cuenta* es un usuario global que también es un usuario de la aplicación de CALM. Una persona puede tener más de una cuenta, cada una de ellas con una función definida por el usuario distinta.

Cumple con FIPS 140-2

Cumple con FIPS 140-2 es una designación para un producto que, de modo predeterminado, utiliza *solamente* algoritmos criptográficos certificados por un laboratorio de pruebas de módulos de cifrado. CA Enterprise Log Manager puede utilizar módulos criptográficos basados en las bibliotecas certificadas RSA BSAFE Crypto-C ME y Crypto-J en modo FIPS, pero no lo puede hacer de forma predeterminada.

descongelación

La *descongelación* es el proceso de modificación del estado de una base de datos de frío a descongelado. El proceso de descongelación se lleva a cabo mediante el servidor de CA Enterprise Log Manager cuando éste recibe una notificación de la utilidad LMArchive de que se ha restaurado una base de datos fría conocida. (Si la base de datos fría no se restaura en el servidor de CA Enterprise Log Manager original, no se empleará la utilidad LMArchive y no será necesario realizar la descongelación; la recatalogación añadirá la base de datos restaurada como base de datos tibia.)

Destinos de traps de SNMP

Se pueden agregar uno o varios *destinos de traps de SNMP* al realizar la programación de una alerta de acción. Cada destino de trap de SNMP se configura mediante un puerto y una dirección IP. El destino suele ser un NOC o un servidor de gestión como CA Spectrum o CA NSM. Se envía un trap de SNMP a los destinos configurados cuando las consultas de una tarea de alerta programada devuelven resultados.

dispositivo de software

Un *dispositivo de software* es un paquete de software completamente funcional que contiene el software, el sistema operativo subyacente y todos los paquetes dependientes. Se instala sobre hardware proporcionado por el usuario final mediante el arranque del medio de instalación de la aplicación de software.

elementos de integración

Los *elementos de integración* incluyen un sensor, un ayudante de la configuración, un archivo de acceso a datos, uno o varios archivos de análisis de mensajes (XMP) y uno o varios archivos de asignación de datos.

enrutador de SAPI

El *enrutador de SAPI* es un adaptador de CA que recibe eventos de integraciones, como la unidad central, y los envía a un enrutador de CA Audit.

entrada de registro

Una *entrada de registro* es la entrada de un registro que contiene información sobre un determinado evento que se ha producido en un sistema o en una red.

entrada de registro

Una *entrada de registro* es un registro de auditoría individual.

estado caliente de base de datos

Un *estado caliente de base de datos* es el estado de la base de datos del sistema de almacenamiento de registro de eventos en la que se insertan los eventos nuevos. Cuando la base de datos caliente alcanza el tamaño configurable en el servidor de recopilación, dicha base de datos se comprime, se cataloga y se traslada al almacenamiento tibio del servidor de informes. Además, todos los servidores almacenan eventos autocontrolados nuevos en una base de datos caliente.

estado descongelado de base de datos

El *estado descongelado de base de datos* es el estado aplicado a una base de datos que se ha restaurado en el directorio de archivo después de que el administrador haya ejecutado la utilidad LMArchive para notificar a CA Enterprise Log Manager de que se ha restaurado. Las bases de datos descongeladas se retienen durante el número de horas configurado en la política de exportación. Puede realizar consultas en registros de eventos de bases de datos en estado caliente, tibio y descongelado.

estado frío de base de datos

El *estado frío de base de datos* se aplica a una base de datos tibia cuando un administrador ejecuta la utilidad LMArchive para notificar al servidor de CA Enterprise Log Manager de que la base de datos tiene una copia de seguridad. Los administradores deben realizar copias de seguridad de las bases de datos tibias y ejecutar esta utilidad antes de que se eliminen. Una base de datos tibia se elimina automáticamente cuando su antigüedad supera el número máximo de días de archivado o cuando se alcanza el umbral de espacio en disco para archivo, lo que suceda en primer lugar. Puede realizar consultas en la base de datos de archivo para identificar las bases de datos en estado tibio o frío.

estados de la base de datos

Los *estados de la base de datos* son los siguientes: caliente para las bases de datos con eventos nuevos no comprimidas; tibio para las bases de datos de eventos no comprimidos; frío para bases de datos con copia de seguridad; y descongelado para las bases de datos restauradas en el sistema de almacenamiento de registro de eventos desde el que se copiaron. Puede realizar consultas en bases de datos calientes, tibias y descongeladas. Una consulta de archivos muestra información de las bases de datos frías.

etiqueta

Una *etiqueta* es una frase clave o un término empleado para identificar consultas o informes pertenecientes al mismo grupo relevante para el negocio. Las etiquetas permiten realizar búsquedas basadas en grupos relevantes para el negocio. Etiqueta también es el nombre del recurso empleado en todas las políticas para permitir a los usuarios crear etiquetas.

event_action

El campo *event_action* es el campo específico del evento de cuarto nivel de la normalización de eventos empleado por la gramática de eventos comunes. Describe acciones comunes. Entre los ejemplos de tipos de acciones de eventos se incluyen los de inicio de proceso, detención de proceso y error de aplicación.

event_category

El campo *event_category* es el campo específico del evento de segundo nivel de la normalización de eventos empleado por la gramática de eventos comunes. Ofrece una mayor clasificación de eventos mediante un campo *ideal_model* específico. Los tipos de categorías de eventos incluyen seguridad operativa, gestión de identidades, gestión de la configuración, acceso a recursos y acceso al sistema.

event_class

El campo *event_class* es el campo específico del evento de tercer nivel de la normalización de eventos empleado por la gramática de eventos comunes. Ofrece una mayor clasificación de eventos mediante un campo *event_category* específico.

evento autocontrolado

Un *evento autocontrolado* es un evento que se registra mediante CA Enterprise Log Manager. Estos eventos se generan de forma automática mediante acciones llevadas a cabo por usuarios registrados y mediante funciones llevadas a cabo por varios módulos, como servicios y escuchas. El informe de detalles de eventos autocontrolados de SIM se puede visualizar seleccionando un servidor de informes y abriendo la ficha Eventos autocontrolados.

evento local

Un *evento local* es un evento que afecta a una sola entidad, mientras que el origen y el destino del evento están en el mismo equipo de host. Un evento local es el tipo 1 de los cuatro tipos de eventos empleados en la gramática de eventos comunes (CEG).

evento nativo

Un *evento nativo* es el estado o la acción que desencadena un evento sin formato. Los eventos nativos se reciben y se analizan/asignan según corresponda y, a continuación, se transmiten como eventos sin formato o refinados. Una autenticación errónea es un evento nativo.

evento observado

Un *evento observado* es un evento que afecta al origen, al destino y al agente. Un agente de recopilación de eventos observa y registra dicho evento.

evento refinado

Un *evento refinado* consta de la información de un evento asignado o analizado derivada de eventos sin formato o resumidos. CA Enterprise Log Manager lleva a cabo la asignación y el análisis de manera que se puedan realizar búsquedas en la información almacenada.

evento registrado

Un *evento registrado* consta de la información de un evento sin formato o refinado tras su inserción en la base de datos. Los eventos sin formato siempre se registran, a no ser que se supriman o se resuman, ya que son eventos refinados. Esta información se almacena y se pueden realizar búsquedas en ella.

evento remoto

Un *evento remoto* es un evento que afecta a dos equipos de host diferentes: el de origen y el de destino. Un evento remoto es el tipo 2 de los cuatro tipos de eventos empleados en la gramática de eventos comunes (CEG).

evento RSS

Un *evento RSS* (del inglés Rich Site Summary) es un evento generado por CA Enterprise Log Manager para transmitir una alerta de acción a usuarios y productos de terceros. El evento consta de un resumen del resultado de cada alerta de acción, así como de un vínculo al archivo de resultados. Se puede configurar la duración de un determinado elemento de fuente RSS.

evento sin formato

Un *evento sin formato* es la información activada por un evento nativo que se envía a través de un agente de control al recopilador del gestor de registros. El evento sin formato se formatea a menudo como cadena de syslog o par de nombre y valor. Se puede revisar un evento en su estado sin formato en CA Enterprise Log Manager.

eventos

Los *eventos* de CA Enterprise Log Manager son las entradas de registro generadas por cada origen de eventos especificado.

explorador de agentes

El *explorador de agentes* es el almacén de los ajustes de la configuración de agentes. (Es posible instalar agentes en un punto de recopilación o en los puntos finales en los que existen orígenes de eventos.)

federación en malla

Una *federación en malla* de servidores de CA Enterprise Log Manager es una topología que establece una relación entre los servidores al mismo nivel. En su estructura más sencilla, el servidor 2 es el servidor secundario del servidor 1, y el servidor 1 es el servidor secundario del servidor 2. Un par de servidores en malla tiene una relación bidireccional. Una federación en malla puede definirse de manera que muchos servidores sean equivalentes entre sí. Una consulta federada arroja resultados del servidor seleccionado y sus equivalentes.

federación jerárquica

Una *federación jerárquica* de servidores de CA Enterprise Log Manager es una topología que establece una relación jerárquica entre los servidores. En su estructura más sencilla, el servidor 2 es el servidor secundario del servidor 1, pero el servidor 1 no es el servidor secundario del servidor 2, es decir, que la relación es unidireccional. Una federación jerárquica puede tener múltiples niveles de relaciones principal-secundario y un solo servidor principal puede tener numerosos servidores secundarios. Una consulta federada arroja resultados del servidor seleccionado y sus servidores secundarios.

filtrado de eventos

El *filtrado de eventos* es el proceso de interrupción de eventos en función de los filtros de la gramática de eventos comunes.

filtro

Un *filtro* es un método que puede emplear para restringir una consulta del sistema de almacenamiento de registro de eventos.

filtro de acceso

Un *filtro de acceso* es un filtro que el administrador puede emplear para controlar qué datos de eventos pueden visualizar los grupos o los usuarios que no son administradores. Por ejemplo, un filtro de acceso puede restringir los datos que pueden ver en un informe las identidades especificadas. Los filtros de acceso se convierten de forma automática en políticas de obligación.

filtro global

Un *filtro global* es un conjunto de criterios que puede especificar y que limita lo que se muestra en todos los informes. Por ejemplo, un filtro global de los eventos de informes de los últimos 7 días generado durante los últimos siete días.

filtro local

Un *filtro local* es un conjunto de criterios que puede establecer mientras visualiza un informe para limitar los datos mostrados en dicho informe.

FIPS 140-2

FIPS 140-2 equivale a los Estándares Federales de Procesamiento de la Información. Estos estándares federales especifican los requisitos de seguridad para los módulos criptográficos que se utilizan en los sistemas de seguridad que protegen información confidencial pero no clasificada. Estos estándares proporcionan cuatro niveles cualitativos de seguridad, diseñados para cubrir un amplio abanico de aplicaciones y entornos potenciales.

función Administrator

La *función Administrator* ofrece a los usuarios la posibilidad de llevar a cabo todas las acciones válidas en todos los recursos de CA Enterprise Log Manager. Los administradores son los únicos que pueden configurar los servicios y la recopilación de registros, así como gestionar usuarios, políticas de acceso y filtros de acceso.

función Analyst

La *función Analyst* ofrece a los usuarios la posibilidad de crear y editar consultas e informes personalizados, editar y anotar informes, crear etiquetas, así como programar informes y alertas de acción. Los analistas también pueden llevar a cabo las tareas de los auditores.

función Auditor

La *función Auditor* ofrece a los usuarios acceso a informes y a los datos que contienen. Los auditores puede visualizar informes, la lista de plantillas de informes, la lista de trabajos de informes programados y la lista de informes generados. Los auditores pueden programar y anotar informes. Los auditores no tienen acceso a las fuentes RSS a no ser que la configuración se establezca para no solicitar ninguna autenticación para visualizar alertas de acción.

función del usuario

Una *función del usuario* puede ser un grupo de usuarios de la aplicación predeterminado o un grupo de aplicaciones definido por el usuario. Es necesario contar con funciones de usuarios personalizadas cuando los grupos de la aplicación predeterminados (Administrator, Analyst y Auditor) no están lo suficientemente depurados como para reflejar las asignaciones de trabajo. Las funciones de usuarios personalizadas requieren el empleo de políticas de acceso personalizado y la modificación de las políticas predefinidas para incluir la función nueva.

gestión de agentes

La *gestión de agentes* es el proceso de software que controla todos los agentes asociados a los servidores de CA Enterprise Log Manager federados. Autentica los agentes que se comunican con este proceso.

gestión de la titularidad

La *gestión de la titularidad* es el método para controlar lo que los usuarios pueden hacer una vez que se autentican e inician sesión en la interfaz de CA Enterprise Log Manager. Esto se logra mediante políticas de acceso asociadas a funciones asignadas a usuarios. Las funciones o grupos de usuarios de la aplicación, así como las políticas de acceso pueden estar predefinidos o definidos por el usuario. El almacén de usuarios interno de CA Enterprise Log Manager es el que realiza la gestión de la titularidad.

gestión de los registros de seguridad de equipos

La *gestión de los registros de seguridad de equipos (Computer Security Log Management)* se define, según el NIST, como "el proceso de generar, transmitir, almacenar, analizar y eliminar datos de registros de seguridad de los equipos".

gramática de eventos comunes (CEG)

La *gramática de eventos comunes (CEG)* es el esquema que ofrece un formato estándar al que CA Enterprise Log Manager convierte los eventos mediante archivos de análisis y asignación antes de almacenarlos en el sistema de almacenamiento de registro de eventos. La gramática de eventos comunes emplea campos comunes y normalizados para definir los eventos de seguridad desde diferentes plataformas y productos. Los eventos que no se pueden analizar o asignar se almacenan como eventos sin formato.

grupo de agentes

Un *grupo de agentes* es una etiqueta que pueden aplicar los usuarios a agentes seleccionados que permite a los usuarios aplicar la configuración de un agente a múltiples agentes a la vez, así como recuperar informes basados en los grupos. Un agente determinado sólo puede pertenecer a un grupo a la vez. Los grupos de agentes se basan en criterios definidos por el usuario, como la región geográfica o la importancia.

grupo de aplicaciones

Un *grupo de aplicaciones* es un grupo específico del producto que se puede asignar a un usuario global. Los grupos de aplicaciones predefinidos para CA Enterprise Log Manager, o funciones, son Administrator, Analyst y Auditor. Estos grupos de aplicaciones sólo están disponibles para usuarios de CA Enterprise Log Manager; no se pueden asignar a usuarios de otros productos registrados en el mismo servidor de CA EEM. Los grupos de aplicaciones definidos por el usuario debe añadirse a la política predeterminada de acceso a la aplicación de CALM para que los usuarios de dichos grupos puedan acceder a CA Enterprise Log Manager.

grupo de usuarios

Un *grupo de usuarios* puede ser un grupo de aplicaciones, un grupo global o un grupo dinámico. Los grupos de aplicaciones de CA Enterprise Log Manager predefinidos son Administrator, Analyst y Auditor. Los usuarios de CA Enterprise Log Manager pueden formar parte de grupos globales a través de pertenencias independientes de CA Enterprise Log Manager. Los grupos dinámicos son grupos definidos por el usuario y creados mediante una política de grupos dinámicos.

grupo dinámico de usuarios

Los *grupos dinámicos de usuarios* constan de usuarios globales que comparten uno o varios atributos. Los grupos dinámicos de usuarios se crean mediante una política de grupo dinámico de usuarios en la que el nombre del grupo dinámico de usuarios y la pertenencia se basan en un conjunto de filtros configurados en los atributos de los usuarios y del grupo.

grupo global

Un *grupo global* es un grupo compartido en las instancias de la aplicación registradas en el mismo servidor de gestión de CA Enterprise Log Manager. Un usuario puede estar asignado a uno o varios grupos globales. Las políticas de acceso se pueden definir en los grupos globales como identidades que pueden o no llevar a cabo acciones seleccionadas en determinados recursos.

ideal_model

ideal_model representa la tecnología que expresa el evento. Este es el primer campo de la gramática de eventos comunes en una jerarquía de campos empleados para la clasificación y la normalización de eventos. Los ejemplos de un modelo ideal incluyen antivirus, DBMS, cortafuegos, sistema operativo y servidor Web. Los productos de cortafuegos Check Point, Cisco PIX y Netscreen/Juniper podrían normalizarse mediante la introducción del valor "Cortafuegos" en el campo *ideal_model*.

identidad

Una *identidad* de CA Enterprise Log Manager es un usuario o un grupo que puede acceder a la instancia de la aplicación de CAELM y a sus recursos. La identidad de los productos de CA puede ser un usuario global, un usuario de la aplicación, un grupo global, un grupo de aplicaciones o un grupo dinámico.

informe

Un *informe* es una pantalla gráfica o en forma de tabla de datos de registro de eventos generada mediante la ejecución de consultas predefinidas o personalizadas con filtros. Los datos pueden proceder de bases de datos calientes, tibias y descongeladas del sistema de almacenamiento de registro de eventos del servidor seleccionado y, si se solicita, de sus servidores federados.

Informes relacionados con EPHI

Los *informes relacionados con EPHI* son informes que se centran en la seguridad de HIPAA; EPHI hace referencia a la información médica protegida electrónicamente. Estos informes pueden ayudarle a demostrar que toda la información sanitaria identificable de forma individual y relacionada con los pacientes que se crea, se mantiene o se transmite electrónicamente está protegida.

Instalador

El *instalador* es la persona que instala el dispositivo de software y los agentes. Durante el proceso de instalación, se crean los nombres de usuario de caelmadmin y EiamAdmin y se asigna a caelmadmin la contraseña especificada para EiamAdmin. Estas credenciales de caelmadmin son necesarias para el primer acceso al sistema operativo; las credenciales de EiamAdmin son necesarias para el primer acceso al software de CA Enterprise Log Manager y para la instalación de agentes.

instancia de la aplicación

Una *instancia de la aplicación* es un espacio común en el repositorio de CA EEM donde se almacenan todas las configuraciones, usuarios, grupos, contenido y políticas de autorización. Normalmente, todos los servidores de CA Enterprise Log Manager de una empresa emplean la misma instancia de la aplicación (CAELM de forma predeterminada). Puede instalar servidores de CA Enterprise Log Manager con diferentes instancias de la aplicación, pero sólo se pueden federar los servidores que compartan la misma instancia de la aplicación. Los servidores configurados para emplear el mismo servidor de CA EEM, pero que tengan instancias de la aplicación diferentes, sólo compartirán el almacén de usuarios, las políticas de contraseñas y los grupos globales. Distintos productos de CA poseen instancias de la aplicación diferentes.

integración

La *integración* es el método a través del cual se procesan los eventos no clasificados para convertirlos en eventos refinados, de manera que se puedan visualizar en consultas e informes. La integración se lleva a cabo a través de un conjunto de elementos que permite a un agente y a un conector determinados recopilar eventos de uno o varios tipos de orígenes de eventos y enviarlos a CA Enterprise Log Manager. El conjunto de elementos incluye el sensor de registro y archivos XMP y de asignación de datos que están diseñados para leer un producto específico. Los ejemplos de integraciones predefinidas incluyen aquellos para el procesamiento de eventos de syslog y eventos WMI. Puede crear integraciones personalizadas para permitir el procesamiento de eventos no clasificados.

lista de control de acceso de identidades

Una *lista de control de acceso de identidades* le permite especificar las diferentes acciones que puede llevar a cabo cada identidad seleccionada en los recursos determinados. Por ejemplo, mediante una lista de control de acceso de identidades, puede especificar que una identidad pueda crear informes y que otra pueda programar y anotar informes. Una lista de control de acceso de identidades se diferencia de una lista de control de acceso en que la primera se centra en las identidades en lugar de centrarse en los recursos.

MIB (base de información gestionada)

La *MIB (base de información gestionada)* de CA Enterprise Log Manager, CA-ELM.MIB, debe importarse y compilarse por parte de cada producto que vaya a recibir alertas en forma de traps de SNMP de CA Enterprise Log Manager. La MIB muestra el origen de cada identificador de objeto (OID) empleado en un mensaje de trap de SNMP con una descripción de dicho objeto de datos o elemento de red. En la MIB de los traps de SNMP enviados por CA Enterprise Log Manager, la descripción textual de cada objeto de datos es para el campo de la gramática de eventos comunes asociada. La MIB permite asegurarse de que todos los pares de nombre/valor enviados en un trap de SNMP se interpretan correctamente en el destino.

MIB personalizada

Una *MIB personalizada* es una MIB creada para una alerta de acción que se envía a un destino de mensaje SNMP, como CA NSM. El ID del mensaje SNMP personalizado que se especifica en la alerta de acción presupone la existencia de una MIB personalizada que defina los campos de la gramática de eventos comunes seleccionados, que se envían como mensaje SNMP.

modo FIPS

El modo FIPS es el valor de configuración que requiere que los servidores y agentes de CA Enterprise Log Manager utilicen módulos criptográficos certificados por FIPS de RSA para el cifrado. El valor de configuración alternativo es el modo no FIPS.

modo no FIPS

Modo no FIPS es el valor de configuración predeterminado que permite que los servidores y agentes de CA Enterprise Log Manager utilicen una combinación de técnicas de cifrado, algunas de las cuales no cumplen con FIPS. El valor de configuración alternativo es el modo FIPS.

módulo (para descargar)

Un *módulo* es un grupo lógico de actualizaciones de componentes disponible para su descarga a través de una suscripción. Un módulo puede contener actualizaciones de archivos binarios, actualizaciones de contenido o ambas. Por ejemplo, todos los informes forman un módulo; todas las actualizaciones de archivos binarios del patrocinador forman otro módulo. CA define los elementos que componen cada módulo.

módulo de suscripción

El *módulo de suscripción* es el servicio que permite que las actualizaciones de suscripción del servidor de suscripciones de CA se descarguen y se distribuyan de forma automática a todos los servidores de CA Enterprise Log Manager y a todos los agentes. La configuración global se aplica a los servidores de CA Enterprise Log Manager locales; la configuración local incluye si el servidor es un proxy sin conexión, un proxy en línea o un cliente de suscripción.

NIST

El *instituto nacional de normas y tecnología (NIST por sus siglas en inglés)* es una agencia estadounidense que ofrece recomendaciones en su publicación especial 800-92, *Guide to Computer Security Log Management* (Guía para la gestión de registros de seguridad de equipos), empleadas como base para CA Enterprise Log Manager.

nombre del usuario EiamAdmin

EiamAdmin es el nombre de superusuario predeterminado asignado al instalador de los servidores de CA Enterprise Log Manager. Al instalar el primer software de CA Enterprise Log Manager, el instalador crea una contraseña para esta cuenta de superusuario, a no ser que ya exista un servidor CA EEM remoto. En ese caso, el instalador debe introducir la contraseña existente. Tras instalar el dispositivo de software, el instalador abre un explorador desde una estación de trabajo, introduce la URL de CA Enterprise Log Manager e inicia sesión como EiamAdmin con la contraseña correspondiente. Este primer usuario define el almacén de usuarios, crea las políticas de contraseñas y crea la primera cuenta de usuario con la función Administrator. El usuario EiamAdmin también puede llevar a cabo cualquier operación controlada por CA EEM.

Objeto seguro

Objeto seguro es un tipo de recurso predefinido de CA EEM. Es la clase de recursos a la que pertenece Objetos aplicación, almacenado en la aplicación. Los usuarios que definen políticas y filtros para permitir el acceso a Objetos aplicación hacen referencia a este tipo de recurso.

Objetos aplicación

Objetos aplicación son recursos específicos del producto almacenados en CA EEM en la instancia de la aplicación de un producto determinado. En el caso de la instancia de la aplicación de CAELM, estos recursos incluyen contenido de consultas e informes, tareas programadas para informes y alertas, configuraciones y contenido de agentes, configuraciones de servicios, adaptadores e integración, archivos de asignación de datos y análisis de mensajes, así como reglas de supresión y resumen.

OID (identificador de objeto)

Un *OID (identificador de objeto)* es un identificador numérico exclusivo para un objeto de datos que se empareja con un valor en un mensaje de trap de SNMP. Cada OID empleado en un trap de SNMP enviado por CA Enterprise Log Manager se asigna a un campo de la gramática de eventos comunes de la MIB. Cada OID asignado a un campo de la gramática de eventos comunes tiene esta sintaxis: 1.3.6.1.4.1.791.9845.x.x.x, donde 791 es el número de empresa de CA y 9845 es el identificador de producto de CA Enterprise Log Manager.

origen de evento

Un *origen de evento* es el host desde el que un conector recopila eventos sin procesar. Un origen de evento puede incluir varios almacenes de registro. A cada uno de ellos se accede mediante un conector independiente. Al implementar un conector nuevo, suele ser necesario configurar el origen de evento, de forma que el agente pueda acceder a éste y leer los eventos sin procesar desde uno de sus almacenes de registro. Los eventos sin procesar del sistema operativo, diferentes bases de datos y varias aplicaciones de seguridad se almacenan por separado en el origen de evento.

perfil

Un *perfil* es un conjunto de filtros de datos y etiquetas opcional y configurable que puede ser específico del producto, específico de la tecnología o aplicado a una categoría seleccionada. Por ejemplo, un filtro de etiquetas para un producto limita las etiquetas listadas a la etiqueta del producto seleccionado. Los filtros de datos de un producto sólo muestran datos del producto especificado en los informes generados, las alertas programadas y los resultados de consultas que visualice. Después de crear el perfil necesario, puede definir que dicho perfil se active siempre que inicie sesión. Si crea varios perfiles, puede aplicar diferentes perfiles (de uno en uno) a las actividades durante una sesión. Los filtros predefinidos se envían con actualizaciones de suscripción.

Petición

Una *petición* es un tipo especial de consulta que muestra los resultados basados en el valor que ha especificado y los campos de la gramática de eventos comunes seleccionados. Sólo se devuelven filas para los eventos en los que el valor especificado aparece en uno o varios campos de la gramática de eventos comunes seleccionados.

política de acceso

Una *política de acceso* es una regla que otorga o deniega a una identidad (usuario o grupo de usuarios) los derechos de acceso a un recurso de la aplicación. CA Enterprise Log Manager determina si las políticas se aplican a un usuario determinado comparando identidades, recursos, clases de recursos, así como evaluando los filtros.

política de acceso a la aplicación de CALM

La *política de acceso a la aplicación de CALM* es un tipo de lista de control de acceso de política de ámbito que define quién puede iniciar sesión en CA Enterprise Log Manager. De forma predeterminada, el administrador [del grupo], el analista [del grupo] y el auditor [del grupo] pueden iniciar sesión.

política de ámbito

Una *política de ámbito* es un tipo de política de acceso que otorga o deniega el acceso a los recursos almacenados en el servidor de gestión, como Objetos aplicación, usuarios, grupos, carpetas y políticas. Una política de ámbito define las identidades que pueden acceder a los recursos especificados.

política de delegación

Una *política de delegación* es una política de acceso que permite a un usuario delegar su autoridad en otro usuario, grupo de aplicaciones, grupo global o grupo dinámico. Debe eliminar de forma explícita las políticas de delegación creadas por el usuario eliminado o desactivado.

política de obligación

Una *política de obligación* es una política creada automáticamente cuando crea un filtro de acceso. No intente crear, editar o eliminar una política de obligación de forma directa. En lugar de ello, cree, edite o elimine el filtro de acceso.

pozFolder

pozFolder es un atributo de Objeto aplicación cuyo valor es la ruta principal de Objeto aplicación. El valor y el atributo *pozFolder* se emplea en los filtros de las políticas de acceso que restringen el acceso a recursos como informes, consultas y configuraciones.

proceso de obtención de resultados de eventos/alertas

El *proceso de obtención de resultados de eventos/alertas* es el proceso de CA IT PAM que solicita a un producto de terceros una respuesta ante datos de alerta configurados en CA Enterprise Log Manager. Puede seleccionar un proceso de CA IT PAM como destino al programar una tarea de alerta. Cuando una alerta ejecuta el proceso de CA IT PAM, CA Enterprise Log Manager envía los datos de alerta de CA IT PAM y CA IT PAM los reenvía con sus propios parámetros de procesamiento al producto de terceros como parte del proceso de obtención de resultados de eventos/alertas.

proceso de valores dinámicos

Un *proceso de valores dinámicos* es un proceso de CA IT PAM que puede activar para rellenar o actualizar la lista de valores de una clave seleccionada empleada en informes o alertas. Ofrezca la ruta al proceso de valores dinámicos como parte de la configuración de IT PAM en la lista de servicios del servidor de informes en la ficha Administración. Haga clic en Importar lista de valores dinámicos en la sección de valores asociada a los valores clave de esa misma página de la IU. La activación del proceso de valores dinámicos es uno de los tres métodos que puede emplear para agregar valores a las claves.

proxy de suscripción (en línea)

Un *proxy de suscripción en línea* es un servidor de CA Enterprise Log Manager con acceso a Internet que obtiene actualizaciones de suscripción del servidor de suscripciones de CA de forma repetitiva. Se puede incluir un determinado proxy de suscripción en línea en la lista de proxys para uno o más clientes, que se ponen en contacto con los proxys de la lista por turnos para solicitar las actualizaciones de archivos binarios. Un determinado proxy en línea, si se configura de este modo, envía contenido nuevo y actualizaciones de configuraciones al servidor de gestión, a no ser que ya los haya enviado otro proxy. El directorio de actualizaciones de suscripción de un proxy en línea seleccionado se emplea como origen para copiar actualizaciones en proxys de suscripción sin conexión.

proxy de suscripción (predeterminado)

El *proxy de suscripción predeterminado* suele ser el servidor de CA Enterprise Log Manager que se ha instalado en primer lugar y también puede ser el servidor de CA Enterprise Log Manager principal. El proxy de suscripción predeterminado también es un proxy de suscripción en línea y, por lo tanto, debe tener acceso a Internet. Si no se define ningún otro proxy de suscripción en línea, este servidor obtiene las actualizaciones de suscripción del servidor de suscripciones de CA, descarga las actualizaciones de archivos binarios para todos los clientes y envía las actualizaciones de contenido a CA EEM. Si se definen otros servidores proxy, este servidor sigue obteniendo actualizaciones de suscripción, pero los clientes sólo se ponen en contacto con él para recibir actualizaciones cuando no se haya configurado ninguna lista de servidores proxy de suscripciones o cuando la lista configurada se haya agotado.

proxy de suscripción (sin conexión)

Un *proxy de suscripción sin conexión* es un servidor de CA Enterprise Log Manager que obtiene actualizaciones de suscripción a través de una copia de directorios manual (mediante scp) de un proxy de suscripción en línea. Los proxys de suscripción sin conexión se pueden configurar para descargar actualizaciones de archivos binarios para clientes que las soliciten y para enviar la versión más reciente de las actualizaciones de contenido al servidor de gestión si aún no las ha recibido. Los servidores proxy de suscripciones sin conexión no necesitan tener acceso a Internet.

proxys de suscripción (para actualizaciones de contenido)

Los *proxys de suscripción para actualizaciones de contenido* son los proxys de suscripción seleccionados para actualizar el servidor de gestión de CA Enterprise Log Manager con actualizaciones de contenido que se descargan desde el servidor de suscripciones de CA. Se recomienda configurar múltiples proxys para disponer de una alternativa en caso de error.

proxys de suscripción (para el cliente)

Los *proxys de suscripción para el cliente* forman la lista de proxys de suscripción con la que se pone en contacto el cliente por turnos para obtener actualizaciones del sistema operativo y del software de CA Enterprise Log Manager. Si un proxy está ocupado, se contacta con el siguiente de la lista. Si no hay ninguno disponible y el cliente está en línea, se emplea el proxy de suscripción predeterminado.

punto de recopilación

Un *punto de recopilación* es un servidor en el que se ha instalado un agente y que tiene una proximidad de red con todos los servidores con orígenes de eventos asociados a los conectores de su agente.

recatalogación

Una *recatalogación* es una reconstrucción forzada del catálogo. La recatalogación sólo es necesaria al restaurar datos en un sistema de almacenamiento de registro de eventos situado en un servidor distinto de aquél en el que se han generado. Por ejemplo, si ha destinado un servidor de CA Enterprise Log Manager para que actúe como punto de restauración para investigaciones en datos fríos, tendrá que forzar una recatalogación de la base de datos tras restaurarla en el punto de restauración designado. La recatalogación se lleva a cabo de manera automática al reiniciar iGateway si es necesario. La recatalogación de un único archivo de la base de datos puede llevar varias horas.

recopilación de eventos

La *recopilación de eventos* es el proceso de lectura de la cadena de eventos sin formato en un origen de eventos y su envío al servidor CA Enterprise Log Manager configurado. La recopilación de eventos va seguida de un refinamiento de eventos.

recopilación directa de registros

La *recopilación directa de registros* es la técnica de recopilación de registros en la que no existe un agente intermedio entre el origen de evento y el software de CA Enterprise Log Manager.

recopilador de SAPI

El *recopilador de SAPI* es un adaptador de CA que recibe eventos de clientes de CA Audit. Los clientes de CA Audit envían con el recopilador una acción que permite una conmutación por error integrada. Los administradores configuran el recopilador de SAPI de CA Audit con, por ejemplo, archivos de asignación de datos y cifrados seleccionados.

recurso de la aplicación

Un *recurso de la aplicación* es cualquiera de los recursos específicos de CA Enterprise Log Manager en los que las políticas de acceso de CALM otorgan o deniegan a determinadas identidades la posibilidad de llevar a cabo acciones específicas de la aplicación como la creación, la programación y la edición. Los ejemplos incluyen los informes, las alertas y las integraciones. Consulte también recurso global.

recurso global

Un *recurso global* del producto de CA Enterprise Log Manager es un recurso compartido con otras aplicaciones de CA. Puede crear políticas de ámbito con recursos globales. Los ejemplos incluyen usuarios, políticas y calendarios. Consulte también recurso de la aplicación.

refinamiento de eventos

El *refinamiento de eventos* es el proceso mediante el cual una cadena de eventos sin formato recopilada se analiza en campos de eventos constitutivos y se asigna a campos de la gramática de eventos comunes. Los usuarios pueden ejecutar consultas para visualizar los datos de eventos refinados resultantes. El refinamiento de eventos es posterior a la recopilación de eventos y anterior al almacenamiento de eventos.

registro

Un *registro* es un registro de auditoría, o un mensaje registrado, correspondiente a un evento o a una recopilación de eventos. El registro puede ser un registro de auditoría, un registro de transacción, un registro de intrusos, un registro de conexión, un registro de rendimiento del sistema, un registro de actividad del usuario o una alerta.

registros de auditoría

Los *registros de auditoría* contienen eventos de seguridad como intentos de autenticación, accesos a archivos y cambios en las políticas de seguridad, las cuentas de usuario o los privilegios. Los administradores especifican qué tipos de eventos deberían auditarse y cuáles se deberían registrar.

reglas de resumen

Las *reglas de resumen* son reglas que combinan determinados eventos nativos del mismo tipo en un evento refinado. Por ejemplo, se puede configurar una regla de resumen para sustituir hasta 1.000 eventos duplicados con los mismos puertos y direcciones IP de origen y destino con un único evento de resumen. Estas reglas simplifican el análisis de eventos y reducen el tráfico de registro.

reglas de supresión

Las *reglas de supresión* son reglas que se configuran para evitar que aparezcan determinados eventos refinados en los informes. Puede crear reglas de supresión permanentes para eliminar eventos de rutina que no supongan problemas de seguridad y puede crear reglas temporales para suprimir el inicio de sesión de eventos planificados como la creación de múltiples usuarios nuevos.

reglas de transferencia de eventos

Las reglas de *transferencia de eventos* indican que los eventos seleccionados deben transferirse a productos de terceros, como aquellos que correlacionan eventos, tras guardarse en el almacén de registro de eventos.

SAPI recorder

Un *SAPI recorder* era la tecnología empleada para enviar información a CA Audit antes de iTechnology. SAPI significa Submit API (interfaz de programación de envío de aplicaciones). Los registradores de CA Audit para CA ACF2, CA Top Secret, RACF, Oracle, Sybase y DB2 son ejemplos de SAPI recorders.

sensor de registro

Un *sensor de registro* es un componente de integración diseñado para leer un tipo de registro específico, como una base de datos, syslog, un archivo o SNMP. Los sensores de registro se reutilizan. Normalmente, los usuarios no crean sensores de registro personalizados.

servicios

Los *servicios* de CA Enterprise Log Manager son el del sistema de almacenamiento de registro de eventos, el del servidor de informes y el de la suscripción. Los administradores configuran estos servicios en un nivel global en el que todos los ajustes se aplican a todos los servidores de CA Enterprise Log Manager de forma predeterminada. La mayor parte de las configuraciones globales de servicios se pueden anular en el nivel local, es decir, para cada servidor de CA Enterprise Log Manager especificado.

servidor de alertas

El *servidor de alertas* es el sistema de almacenamiento de alertas de acción y tareas de alertas de acción.

servidor de almacenamiento remoto

Un *servidor de almacenamiento remoto* es una función asignada a un servidor que recibe bases de datos almacenadas de forma automática de uno o varios servidores de informes. Un servidor de almacenamiento remoto almacena bases de datos frías durante la cantidad de años necesaria. El host remoto empleado para el almacenamiento no suele tener instalado ningún servidor de CA Enterprise Log Manager ni otros productos. Para el almacenamiento automático, configure la autenticación no interactiva.

servidor de gestión

El *servidor de gestión* es una función asignada al primer servidor de CA Enterprise Log Manager instalado. Dicho servidor de CA Enterprise Log Manager contiene el repositorio que almacena el contenido compartido, como las políticas, de todos los servidores de CA Enterprise Log Manager. Este servidor suele ser el proxy de suscripción predeterminado. Aunque no es recomendable para la mayoría de los entornos de producción, el servidor de gestión puede llevar a cabo todas las funciones.

servidor de informes

Un *servidor de informes* es una función desempeñada por un servidor de CA Enterprise Log Manager. Un servidor de informes recibe bases de datos tibias almacenadas de forma automática de uno o varios servidores de recopilación. Un servidor de informes gestiona consultas, informes, alertas programadas e informes programados.

servidor de informes

El *servidor de informes* es el servicio que almacena información de la configuración, como el servidor de correo electrónico que se debe emplear al enviar alertas por correo electrónico, el aspecto de los informes guardados en formato PDF y la retención de políticas para informes guardadas en el servidor de informes y para alertas enviadas a la fuente RSS.

Servidor de ODBC

El *servidor de ODBC* es el servicio configurado que define el puerto empleado para las comunicaciones entre el cliente de ODBC o JDBC y el servidor de CA Enterprise Log Manager, al tiempo que indica si se debe emplear el cifrado SSL.

servidor de punto de restauración

Un *servidor de punto de restauración* es una función desempeñada por un servidor de CA Enterprise Log Manager. Para investigar eventos "fríos", puede desplazar bases de datos del servidor de almacenamiento remoto al servidor de punto de restauración con una utilidad, agregar las bases de datos al catálogo y, a continuación, realizar las consultas. El desplazamiento de bases de datos frías a un punto de restauración dedicado es una alternativa a su desplazamiento al servidor de informes original para su investigación.

servidor de recopilación

Un *servidor de recopilación* es una función desempeñada por un servidor de CA Enterprise Log Manager. Un servidor de recopilación refina los registros de eventos entrantes, los introduce en la base de datos caliente, comprime la base de datos caliente y la copia o la guarda de forma automática en el servidor de informes correspondiente. El servidor de recopilación comprime la base de datos caliente cuando ésta alcanza el tamaño configurado y la almacena de forma automática según la programación configurada.

servidor de suscripciones de CA

El *servidor de suscripciones de CA* es el origen de las actualizaciones de suscripción de CA.

servidor proxy HTTP

Un *servidor proxy HTTP* es un servidor proxy que actúa como cortafuegos y evita que entre o salga tráfico de Internet de la empresa, salvo el que lo hace a través del proxy. El tráfico de salida puede especificar un ID y una contraseña para omitir el servidor proxy. Se puede configurar el empleo de un servidor proxy HTTP local en la gestión de suscripciones.

servidores de federación

Los *servidores de federación* son servidores de CA Enterprise Log Manager conectados entre sí en una red con el objetivo de distribuir la recopilación de los datos de registro, al tiempo que acumulan los datos recopilados para generar informes. Los servidores de federación se pueden conectar en una topología jerárquica o en malla. Los informes de datos federados incluyen los del servidor de destino, así como los de los secundarios o equivalentes, si los hay, de dicho servidor.

SNMP

SNMP es el acrónimo de protocolo simple de administración de redes (Simple Network Management Protocol), un estándar abierto para el envío de mensajes de alerta en forma de traps de SNMP desde un sistema de agente a uno o varios sistemas de gestión.

supresión

La *supresión* es el proceso de interrupción de eventos en función de los filtros de la gramática de eventos comunes. La supresión se lleva a cabo mediante archivos de supresión.

token de análisis de mensajes (ELM)

Un *token de análisis de mensajes* es una plantilla reutilizable para crear la sintaxis de expresión regular empleada en el análisis de mensajes de CA Enterprise Log Manager. El token tiene un nombre, un tipo y una cadena de expresión regular correspondiente.

URL de fuente RSS para alertas de acción

La *URL de fuente RSS para alertas de acción* es:
<https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp>. En esta URL, puede visualizar alertas de acción sujetas a la configuración de cantidad y antigüedad máximas.

URL de fuente RSS para suscripción

La *URL de fuente RSS para suscripción* es un vínculo preconfigurado empleado por los servidores proxy de suscripción en línea durante el proceso de recuperación de actualizaciones de suscripción. Esta URL es para el servidor de suscripciones de CA.

URL para CA Embedded Entitlements Manager

La *URL para CA Embedded Entitlements Manager* (CA EEM) es:
https://<ip_address>:5250/spin/eiam. Para iniciar sesión, seleccione CAELM como aplicación e introduzca la contraseña asociada al nombre de usuario de EiamAdmin.

URL para CA Enterprise Log Manager

La *URL para CA Enterprise Log Manager* es:
https://<ip_address>:5250/spin/calm. Para iniciar sesión, introduzca el nombre de usuario definido en su cuenta por el administrador y la contraseña correspondiente. También puede introducir EiamAdmin, el nombre de superusuario predefinido, con la contraseña correspondiente.

usuario de EEM

El *usuario de EEM*, configurado en la sección de almacenamiento automático del sistema de almacenamiento de registro de eventos, especifica el usuario que puede realizar una consulta de archivo, recatalogar la base de datos de archivo, ejecutar la utilidad LMArchive y ejecutar el script shell restore-ca-elm para restaurar bases de datos almacenadas para su examen. A este usuario se le debe asignar la función predeterminada de administrador o una función personalizada asociada a una política personalizada que permita la acción de edición en un recurso de la base de datos.

usuario de la aplicación

Un *usuario de la aplicación* es un usuario global al que se han asignado detalles en el ámbito de la aplicación. Los detalles del usuario de la aplicación de CA Enterprise Log Manager incluyen el grupo de usuarios y cualquier restricción del acceso. Si el almacén de usuarios es el repositorio local, los detalles del usuario de la aplicación también incluyen las credenciales de inicio de sesión y las políticas de contraseñas.

usuario global

Un *usuario global* es la información de cuenta de usuario que excluye los detalles específicos de la aplicación. Los detalles de usuarios globales y las pertenencias a grupos globales se comparten en todas las aplicaciones de CA que se integran en el almacén de usuarios predeterminado. Los detalles de usuarios globales se pueden almacenar en el repositorio o en un directorio externo.

utilidad LMArchive

La *utilidad LMArchive* es la utilidad de línea de comandos que realiza el seguimiento de la copia de seguridad y la restauración de bases de datos de archivo en el sistema de almacenamiento de registro de eventos de un servidor de CA Enterprise Log Manager. Utilice LMArchive para realizar consultas de la lista de archivos de bases de datos tibias que están listos para su almacenamiento. Tras realizar una copia de seguridad de la base de datos listada y trasladarla al almacenamiento a largo plazo (frío), utilice LMArchive para crear un registro en el servidor de CA Enterprise Log Manager en el que se realizó la copia de seguridad de dicha base de datos. Tras restaurar la base de datos fría en su servidor de CA Enterprise Log Manager original, utilice LMArchive para notificar a CA Enterprise Log Manager, quien, a su vez, cambia el estado de los archivos de la base de datos a estado descongelado para que se puedan emplear en las consultas.

utilidad LMSEOSImport

La utilidad *LMSEOSImport* es una utilidad de línea de comandos empleada para importar SEOSDATA, o eventos existentes, en el servidor de CA Enterprise Log Manager como parte de la migración de Audit Reporter, Viewer o Audit Collector. Esta utilidad sólo es compatible con Microsoft Windows y Sun Solaris Sparc.

utilidad scp

La copia segura *scp* (programa de copia de archivos remota) es una utilidad de UNIX que transfiere archivos entre equipos de UNIX de una red. Esta utilidad está disponible al realizar la instalación de CA Enterprise Log Manager con el objetivo de emplearla para transferir archivos de actualización del proxy de suscripción en línea al proxy de suscripción sin conexión.

valores de clave

Los *valores de clave* son valores definidos por el usuario y asignados a una lista definida por el usuario (grupo de claves). Cuando una consulta emplea un grupo de claves, los resultados de la búsqueda incluyen las coincidencias con cualquiera de los valores de clave del grupo de claves. Existen varios grupos de claves predefinidos; algunos de ellos incluyen valores de clave predefinidos que se emplean en las consultas y los informes predefinidos.

varbind

Una *varbind* es un enlace variable SNMP. Cada varbind se constituye de un OID, un tipo, y un valor. Las varbinds se agregan a las MIB personalizadas.

Índice

A

- accesibilidad - 701
- adaptadores de CA
 - definido - 182
 - editar - 183, 184
 - visualizar el estado - 186
- agentes
 - actualizar - 687
 - actualizar claves de autenticación - 667
 - aplicar actualizaciones - 687
 - asignar gestores - 680
 - crear un grupo - 677
 - planificar - 657, 661
- alertas de acción
 - activación - 500
 - configurar retención - 496
 - crear filtros avanzados - 597
 - definido - 372
 - definir destino de tarea de alerta - 485
 - editar - 499
 - ejecución de un proceso de IT PAM por consulta - 426
 - ejecución de un proceso de IT PAM por fila - 421
 - ejemplos - 486, 490
 - eliminar - 501
 - notificación de correo electrónico - 480
 - uso de etiquetas y consultas - 373
- almacenamiento de registros
 - crear una copia de seguridad - 217
 - restaurar una copia de seguridad - 221, 228
- análisis de mensajes
 - analizar archivos - 576
 - cargar eventos de ejemplo - 562
 - crear - 558
 - definido - 558
 - definir detalles de archivo - 560
 - filtros de coincidencia previa - 564
 - proceso de creación de archivos - 558
- árbol de MIB

- para CA-ELM MIB - 432
- para MIB personalizada - 446
- asignación de datos
 - analizar archivos - 591
 - asignaciones de bloque - 589
 - crear - 577
 - definido - 558
 - función concat - 586
 - proceso de creación de archivos - 577

B

- bases de datos archivadas
 - crear una copia de seguridad - 219
 - listar sin copia de seguridad - 217
 - registrar la copia de seguridad - 219
 - registrar la restauración - 226
- biblioteca de refinamiento de eventos
 - versiones de componentes - 527

C

- CA Enterprise Log Manager
 - eliminar tras desinstalar - 153
 - modo de accesibilidad - 701
- calendario
 - agregar a una política - 115
 - crear - 113
 - ejemplo - 116
- catálogo de archivado
 - reconstruir (recatalogar) - 231
- certificado de raíz de confianza
 - agregación a iAuthority - 694
 - agregación a iControl - 696
- certificados, personalización
 - implementación - 693
 - implementar - 698
 - raíz de confianza - 694
- clave de autenticación del agente
 - actualizar - 667
- condiciones del resultado
 - condiciones de grupo - 514
 - configurar - 511

- definido - 511
- conectores
 - abrir lista - 688
 - aplicar actualizaciones de integraciones - 687
 - editar - 629
 - petición - 298
 - visualizar - 627
- configuración global
 - servicios - 157
- consultas
 - agregar informe de obtención de detalles - 330
 - condiciones del resultado - 511, 514
 - desactivar visualización automática - 332
 - editar - 331
 - eliminar - 331
 - exportar detalles - 333
 - filtros avanzados - 509
 - importar detalles - 334
 - modo de edición - 332
 - personalización para alertas de acción - 376
- contraseña de usuario
 - cambiar - 27
 - restablecer - 48
- cuentas de usuario, referenciadas
 - administrar - 44
- cuentas de usuarios
 - activar y desactivar - 44
 - administrar automáticamente - 25
 - agregar un grupo de usuarios de la aplicación - 42
 - configurar con ajustes predeterminados - 39
 - crear - 41
 - desbloquear - 26
 - editar - 45
 - ejemplo de adición de un grupo de usuarios de la aplicación - 144
 - ejemplo de creación - 127
 - eliminar - 49

E

- ejemplos
 - alerta de espacio en disco bajo - 486

- alerta de evento autocontrolado - 490
- alerta mediante valor keyed de orígenes críticos para el negocio - 497
- calendario - 116
- correo electrónico para el administrador cuando se detiene el flujo de eventos - 493
- envío de mensajes SNMP a CA Spectrum - 456
- federación e informes federados - 341
- informe de consultas existentes - 338
- informes basados en etiqueta de PCI - 291
- planificar instalación de agentes - 657
- políticas para acceso a reglas de asignación y análisis - 146
- políticas para acceso a reglas de supresión y resumen - 148
- políticas para analista de PCI - 139
- políticas para un administrador de Windows - 125
- proceso IT PAM, ejecución manual - 415
- proceso IT PAM, ejecución por consulta con alerta - 426
- proceso IT PAM, ejecución por fila con alerta - 421
- programar informes con una etiqueta común - 517
- programar informes enviados por correo electrónico como PDF - 521
- regla de supresión - 552
- retención de informes - 347
- escuchas de eventos
 - definido - 182
 - editar configuraciones globales - 183
 - editar configuraciones locales - 184
 - enrutador WMI - 664
 - iTechnology - 189
 - SAPI - 187
- estados de la base de datos de registro de eventos - 196
- etiquetas
 - usar en organización de informes - 281
- eventos
 - autocontrol - 524, 525

- creación de una consulta para recuperar graves, - 379
- personalización de una consulta para recuperar graves, - 381
- resumir - 536
- suprimir - 530
- eventos autocontrolados
 - definido - 524
- explorador del agente
 - usar - 665
- exportación
 - detalles de consulta - 333
 - detalles de informes - 348
 - integraciones - 623
 - políticas de acceso - 118
 - reglas de resumen y supresión - 551

F

- federación
 - aplicar a tareas de informes - 506
 - ejemplo - 341
- filtros
 - agregar a informes programados - 504
 - avanzados - 509
 - crear avanzados - 597
 - editar global - 274
 - eliminar global - 274
 - identificación, para eventos graves - 377
- filtros de acceso
 - crear - 111
 - ejemplo de creación - 133
 - eliminar - 120

G

- gestión de suscripciones
 - clave pública - 250
 - requisitos de espacio en disco - 249
- gestión de usuarios y accesos
 - crear filtros de acceso - 111
- gramática de eventos comunes (CEG)
 - asignar y analizar - 558
 - filtrar para ver campos de la gramática de eventos comunes - 509
- grupo de usuarios

- dinámico - 109
- global - 40
- grupo global
 - crear - 40

I

- importación
 - detalles de consulta - 334
 - detalles de informe en tiempo real - 349
 - integraciones - 622
 - proceso de CA IT PAM, ejemplo - 400
 - reglas de resumen y supresión - 550
- informes
 - anotar generado - 505
 - crear - 335, 338
 - crear diseños - 337
 - desactivar visualización automática - 290
 - editar - 346
 - ejemplo - 291
 - eliminar - 346
 - establecer modo de edición - 290
 - etiquetas - 281
 - exportar detalles de informes - 348
 - importar detalles de informes - 349
 - modo de edición - 290
 - obtener detalles - 330
 - programar - 506, 517
 - ver generado - 503
 - visualización - 288
- informes, administración
 - crear informes nuevos - 335
 - programar tareas de informes - 506
 - visualizar informes generados - 503
- instalación del agente
 - planificación - 657
- integración con CA IT PAM
 - configuración para generación de valores dinámicos - 353
 - funcionamiento - 395
- integración con CA NSM
 - requisitos del sistema - 461
- integración con CA Spectrum
 - para traps de SNMP - 166
 - referencia - 451

- integraciones
 - definido - 603
 - exportar - 623
 - importar - 622
 - registro de archivos - 610

L

- listas con clave
 - creación de una alerta con - 497

M

- mensajes SNMP
 - árbol de MIB para, - 432
 - configuración como destino de la alerta - 479
 - configuración de integración - 166
 - contexto de uso - 429
 - descripción - 429
 - ejemplo - 456
 - envío a CA Spectrum - 456
 - visualización en CA NSM - 470
 - visualización en CA Spectrum - 460
- MIB (CA-ELM.MIB)
 - contenido - 432
 - descarga - 454
 - Importación a CA Spectrum - 455
 - ubicación - 447
- MIB personalizada
 - descripción - 439
 - directrices para la creación - 441
 - ejemplo - 444
 - mejores prácticas - 433
 - uso - 447

P

- perfiles
 - configurar - 270
 - crear - 265
 - descripción - 264
- peticiones
 - conector - 298
 - definido - 296
 - dirección IP - 303
 - host - 301

- nombre de registro - 306
- puerto - 308
- usuario - 310
- política de grupos dinámicos de usuarios - 109
- políticas de acceso
 - agregar una identidad - 98
 - comprobar - 108
 - copia de seguridad - 65
 - crear a partir de una copia - 106
 - definido - 52
 - editar - 137, 142
 - ejemplo de creación a partir de una copia - 143
 - ejemplo de creación desde el principio - 129
 - ejemplo definido por el usuario - 129
 - eliminar - 119
 - evaluar impacto - 144
 - exportar - 118
 - planificar - 91, 140
 - política de acceso a la aplicación de CALM - 96
 - predefinidas para los Administrators - 62
 - predefinidas para los Analysts - 59
 - predefinidas para los Auditors - 57
 - predefinidas para todos los usuarios - 53
 - productos registrados - 64
- proceso de salida de alerta/evento
 - CA Service Desk - 402
 - crear - 407
 - diseño de consultas para, - 419
 - ejecución en el resultado de una consulta seleccionada - 415
 - especificación como destino de la alerta - 393
 - flujo de datos para, ejemplo - 398
 - flujo de trabajo para aprovechamiento - 393
 - garantizar la conformidad con, - 407
- programación de informes
 - consultas federadas - 517
 - destino - 517
 - editar - 522
 - eliminar - 524
 - proceso - 506
 - repetición - 515

puertos

petición - 308

R

recopilación de registros

directo - 662

mediante agente - 664

planificar - 661

sin agente - 664

reglas de resumen

aplicar - 543

configurar visualización - 541

crear reglas - 536

establecer umbrales - 537

reglas de supresión

aplicar - 543

asignar nombre - 531

crear - 530

efectos - 529

restricción de acceso, escenario

analista PCI o GRUPO - 139

usuario Win-Admin - 125

rol de usuario

Administrator - 31

Analyst - 30

Auditor - 28

planificar - 90

roles de usuario

asignar - 42

crear - 95

ejemplo de adición a política - 98, 142

ejemplo de asignación - 144

ejemplo de concesión de acceso a la
aplicación - 142

ejemplo de creación - 141

en tareas de creación de informes - 335

garantizar acceso a la aplicación - 96

S

sensores de registros

archivo - 610

servicios

editar configuraciones locales - 158

servicios de escucha - 182

servidor local

configurar - 158

supresión y resumen

aplicar una regla - 543

copiar una regla - 547

definido - 528

editar reglas - 548

eliminar reglas - 549

exportar reglas - 551

importar reglas - 550

syslog

configuraciones predeterminadas - 617

zonas horarias - 619

T

tareas de administración

gestión de agentes - 666

integración de productos - 558

integraciones - 603

políticas de resumen - 536

políticas de supresión - 530

tareas de informes

editar - 522

eliminar - 524

filtrar - 504

filtros avanzados - 509

programar - 506

U

utilidad LMArchive - 232

V

valores dinámicos

activación de importación - 351

configuración de la integración de IT PAM
para, - 353

descripción - 351

generación con un proceso de IT PAM - 352

versiones

definido - 527

regla de resumen y supresión - 548

visores de eventos

visualizar el estado - 186

visualizar eventos autocontrolados - 185