

CA Service Desk Manager

Guida all'implementazione
r12.5



La presente documentazione ed ogni relativo programma software di ausilio (di seguito definiti "Documentazione") vengono forniti unicamente a scopo informativo e sono soggetti a modifiche o ritiro da parte di CA in qualsiasi momento.

La Documentazione non può essere copiata, trasferita, riprodotta, divulgata, modificata o duplicata per intero o in parte, senza la preventiva autorizzazione scritta di CA. La Documentazione è di proprietà di CA e non può essere divulgata dall'utente o utilizzata se non per gli scopi previsti in uno specifico accordo di riservatezza tra l'utente e CA.

Fermo restando quanto sopra, gli utenti licenziatari del software della Documentazione, hanno diritto di effettuare un numero ragionevole di copie della suddetta Documentazione per uso personale e dei propri dipendenti, a condizione che su ogni copia riprodotta siano apposti tutti gli avvisi e le note sul copyright di CA.

Il diritto ad effettuare copie della Documentazione è limitato al periodo di durata della licenza per il prodotto. Qualora a qualsiasi titolo, la licenza dovesse essere risolta da una delle parti o qualora la stessa dovesse giungere a scadenza, l'utente avrà la responsabilità di certificare a CA per iscritto che tutte le copie, anche parziali, del software sono state restituite a CA o distrutte.

FATTO SALVO QUANTO PREVISTO DALLA LEGGE VIGENTE, QUESTA DOCUMENTAZIONE VIENE FORNITA "AS IS" SENZA GARANZIE DI ALCUN TIPO, INCLUDENDO, A TITOLO ESEMPLIFICATIVO, LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ, IDONEITÀ AD UN DETERMINATO SCOPO O DI NON VIOLAZIONE DEI DIRITTI ALTRUI. IN NESSUN CASO CA SARÀ RITENUTA RESPONSABILE DA PARTE DELL'UTENTE FINALE O DA TERZE PARTI PER PERDITE O DANNI, DIRETTI O INDIRETTI, DERIVANTI DALL'UTILIZZO DELLA DOCUMENTAZIONE, INCLUSI, IN VIA ESEMPLIFICATIVA E NON ESAUSTIVA, PERDITE DI PROFITTI, INTERRUZIONI DI ATTIVITÀ, PERDITA DEL VALORE DI AVVIAMENTO O DI DATI, ANCHE NEL CASO IN CUI CA VENGA ESPRESSAMENTE INFORMATA DI TALI PERDITE O DANNI.

L'utilizzo di qualsiasi altro prodotto software citato nella Documentazione è soggetto ai termini di cui al contratto di licenza applicabile, il quale non viene in alcun modo modificato dalle previsioni del presente avviso.

Il produttore di questa Documentazione è CA.

La presente Documentazione viene fornita con "Diritti limitati". L'uso, la duplicazione o la divulgazione da parte del governo degli Stati Uniti è soggetto alle restrizioni elencate nella normativa FAR, sezioni 12.212, 52.227-14 e 52.227-19(c)(1) - (2) e nella normativa DFARS, sezione 252.227-7014(b)(3), se applicabile, o successive.

Copyright © 2010 CA. Tutti i diritti riservati. Tutti i marchi, le denominazioni sociali, i marchi di servizio e i loghi citati in questa pubblicazione sono di proprietà delle rispettive società.

Riferimenti ai prodotti CA

La presente documentazione fa riferimento ai seguenti prodotti CA:

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

Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo <http://www.ca.com/worldwide>.

Sommario

Capitolo 1: Introduzione 15

Panoramica	15
Destinatari	15
Elenco utenti predefiniti di CA Service Desk Manager	16
Componenti server primari o secondari	17

Capitolo 2: Aggiornamento 23

Pianificazione dell'aggiornamento	23
Considerazioni sui database	24
Mantenimento delle personalizzazioni	27
Considerazioni sulla migrazione LREL	30
Considerazioni sulle transizioni di stato	32
Aggiornamento della posta elettronica	32
Funzionamento della console di migrazione	35
File di registro della migrazione	36
Avvio manuale della migrazione	36
Modalità di aggiornamento di CA CMDB da una versione precedente	37
Migrazione di dati Automazione supporto	40
Modalità di migrazione di un database di Automazione supporto	40
Modalità di conversione di divisioni in titolari	41
Esportazione di dati CA Automazione supporto	42
Importazione di dati Automazione supporto	44
Modalità di configurazione dell'accesso previsto dal ruolo di Automazione supporto dopo la migrazione	44
Modalità di migrazione di un universo CA Business Intelligence personalizzato	45
Modalità di esecuzione del backup di un universo personalizzato	45
Installazione di un universo CA Business Intelligence	46
Aggiornamento del collegamento a un universo	46
Configurazione post aggiornamento	47
Modalità di aggiornamento di CA Workflow e CA EEM	47
Cancellazione dei dati nella cache del motore Web e del browser	48
Configurazione di directory e server Web	48
Attività successive alla migrazione LREL	49
Modifica dei tipi accesso	52
Abilitare Calcolo priorità	53
Modalità di aggiunta del campo Priorità incidente agli incidenti	54
Aggiunta del campo Urgenza ai ticket dipendente	55

Modalità di impostazione dei valori del ticket per gli utenti self-service	55
Attivazione di transizioni di stato	58
Attivazione di tipi di transizione	59
Personalizzazione di aree di accesso funzionali	60
File SITEMODS.JS	62
Regolazione dei tipi di accesso	62
Regolazione di impostazioni di partizione dati	63
Modifica dei set di file della Guida dopo la migrazione dei ruoli	64
Impostazioni predefinite dei vincoli	65
Avviare l'interfaccia Web IIS (CAisd)	66
Modalità di aggiornamento di Gestione delle informazioni da r11.2	66
Modalità di aggiornamento di Gestione delle informazioni da r12 o r12.1	68

Capitolo 3: Pianificazione

71

Elenco delle porte predefinite e consigliate di CA Service Desk Manager	71
Pianificazione dell'installazione <MDB>	74
Considerazioni su CA MDB	75
Pianificazione dell'installazione <USDK>	78
Considerazioni su USDK	81
Pianificazione dell'installazione di CA EEM e CA Workflow	92
Considerazioni su CA EEM	94
Considerazioni su CA Workflow	94
Pianificazione dell'integrazione di CA IT PAM	101
Considerazioni sulla protezione	101
Modalità di impostazione delle comunicazioni SSL con CA IT PAM	102
Pianificazione dell'installazione di CA Business Intelligence	105
Considerazioni sulla segnalazione	106
Procedure ottimali del reporting	110
Pianificazione dell'installazione di CA NSM	110
Pianificazione dell'installazione di FAST ESP	111
Strategie di implementazione	112
Abilitazione dell'autenticazione Windows in Firefox	113

Capitolo 4: installazione

115

Modalità di Implementazione del software	115
Installazione dell'CA MDB	116
Installazioni MDB	117
Ricerca dell'integrazione di prodotto e delle informazioni di compatibilità	117
Installazione in SQL Server (Windows)	118
Installazione in Oracle (Windows)	120
Installazione in Oracle (Linux\UNIX)	121

Installazione di CA Service Desk Manager	122
Installazione su SQL Server (Windows)	123
Installazione su Oracle (Windows)	125
Installazione su Oracle (Linux\UNIX)	129
Configurazione di Visualizer	131
Modalità di configurazione di Visualizer in un server secondario	131
Configurazione dei componenti Automazione supporto	132
L'installazione di Screen Painter Web	136
Installazione di Screen Painter Web	136
Installazione dell'integrazione di CA NSM	137
Installazione dell'integrazione di CA NSM (Windows)	137
Installazione di CA EEM	138
Installazione di CA EEM (Windows)	139
Installazione di CA EEM (UNIX)	140
Installazione di CA Workflow	142
Installazione di CA Workflow (Windows)	143
Installazione di CA Workflow (UNIX)	144
Installazione di CA Workflow IDE standalone	145
Disinstallare il client CA Workflow IDE (Windows e Linux)	146
Installazione di ADT	147
Installazione di ADT	147
L'installazione di Federation Adapters di CA CMDB	148
Creazione dell'ID amministratore (SQL Server)	149
Configurazione di ADT (SQL Server)	150
Creazione dell'ID amministratore e configurazione di ADT (Oracle)	151
Installazione dei Federation Adapters di CA CMDB	152
Installazione di FAST ESP	153
Installazione di FAST ESP (Windows)	153
Installazione di FAST ESP (Linux)	154
Il registro di installazione di FAST ESP	155
Installazione di LinguisticsStudio	156
Installazione di CA Business Intelligence	157
Installazione nuova di CA Business Intelligence	158
Installazione personalizzata di CA Business Intelligence (Windows)	159
Verifica dell'installazione	163
Il registro di installazione	164

Capitolo 5: Configurazione	165
Configurazione del prodotto	165
Configurazione dei componenti CA Service Desk Manager	166
Impostazione del registro di controllo di CA CMDB	167
Modalità di integrazione di CA Cohesion ACM con CA CMDB	167

Configurazione di CA CMDB Visualizer su AIX	168
Modifica di script di terze parti per la compatibilità CA CMDB	168
Modalità di passaggio a un altro server di destinazione per CA CMDB Reports	169
Modalità di configurazione dell'interfaccia Web	169
Abilitazione del motore Web sul server secondario (Windows)	170
Abilitazione del motore Web sul server secondario (UNIX)	171
Configurazione dell'interfaccia Web	172
Avvio dell'interfaccia Web	172
Modalità di configurazione di CA Business Intelligence	173
Configurazione delle impostazioni iniziali di CA Business Intelligence	174
Modalità di configurazione dei valori di intervallo di date e dei parametri di join	177
Aggiunta di utenti CA Service Desk Manager alla CMC	178
Aggiungere l'utente privilegiato CA Service Desk Manager a CMC	180
Impostazioni predefinite nella CMC	181
Integrazione di CA Business Intelligence con CA Service Desk Manager	182
Modalità di configurazione dell'autenticazione sicura con CA Service Desk Manager e BusinessObjects	184
Configurazione dell'autenticazione LDAP di BusinessObjects	186
Connessione del server di CA Business Intelligence ad un server di CA Service Desk Manager diverso	187
Cambiamento della dimensione massima di un elenco di valori	190
Cambiamento dei limiti del record del report	191
Cambiamento del valore di timeout della sessione di Web Intelligence	191
Database replicato per il reporting non in linea	192
Esecuzione delle Norme automatiche	193
Esecuzione della scheda Report della conoscenza	194
Importazione di dati di esempio di Gestione delle informazioni	194
Modalità di configurazione di FAST ESP	195
Utilizzo del motore di ricerca FAST	196
Ricerca in repository esterni	197
Cambiamento della strategia di lemmatizzazione	200
Configurazione dei sinonimi	203
Ricerche Argomenti correlati	204
pdm_k_reindex—Utilità di reindicizzazione della conoscenza	205
Utilizzo di pdm_k_reindex con FAST ESP	206
Aumento delle capacità di ricerca	208
Modalità di esecuzione del backup dei dati di FAST ESP	208
Integrazione di FAST ESP nel server secondario	209
Modalità di configurazione di CA Workflow	210
Avvio e arresto di CA Workflow	211
Impostazione dell'accesso automatico (autenticazione esterna)	214
Configurazione di Gestione elenco di lavoro e Gestione flusso di lavoro per l'accesso automatico.	216

Configurazione di Workflow Design Environment per l'accesso automatico	217
Opzioni del flusso di lavoro CA	218
Modalità di configurazione del flusso di lavoro di esempio per Gestione dei problemi.....	219
Modalità di configurazione del flusso di lavoro di esempio per Ordine computer	221
Esempio di modifica delle definizioni del processo di gestione	222
Modalità di configurazione dell'integrazione del flusso di lavoro di CA IT PAM	226
Verificare le installazioni di CA IT PAM e CA Service Desk Manager	227
Configurazione delle opzioni del flusso di lavoro di CA IT PAM	227
Amministrazione utente CA IT PAM.....	230
Modalità di supporto del Single Sign-On da CA Service Desk Manager a CA IT PAM mediante CA EEM.....	232
Impostazione dell'accesso automatico (autenticazione CA MDB)	233
Configurazione di punti di ingresso singoli	235
Modalità di implementazione della funzione multi-tenancy	236
Abilita Multi-Tenancy	239
Modalità di esportazione e importazione di dati di titolari	247
Utilità utilizzate per la funzione multi-tenancy	249

Capitolo 6: Personalizzazione 259

Panoramica sulla personalizzazione	259
Personalizzazione del metodo di notifica.....	260
Processo di notifica	260
Variabili del metodo di notifica	261
Modalità di creazione di un metodo di notifica personalizzato	265
Personalizzazione di query e messaggi	268
Query del segnapunti	269
Query specifiche di ITIL	276
Personalizzazione dei messaggi di notifica delle attività	276
Personalizzazione dello schema	282
Modalità di modifica di Progettazione schema	283
Visualizzazione dello strumento Progettazione schema Screen Painter Web	284
Schede di Progettazione schema	285
Attività di Progettazione schema	290
Personalizzazione dell'interfaccia Web	297
Il Screen Painter Web (WSP)	299
Modelli HTML (moduli HTML)	316
Tag HTML	321
Variabili del server	343
Operazioni del server	350
Personalizzazione avanzata	358
Personalizzazione della memorizzazione dei dati del registro eventi	387
Personalizzazione dei report di CA Business Intelligence	389

Infrastruttura di CA Business Intelligence	390
Ambiente di sviluppo	391
Struttura	393
Cambiamenti dello schema all'infrastruttura	396
Strutture di cartella e report	399
Spostare i nuovi Crystal Report in CA Business Intelligence	403
Modalità di spostamento in CA Business Intelligence dei report di accesso esistenti	405
Passaggio da sviluppo a produzione	405
Personalizzazione di rapporti legacy	406
Progettazione report personalizzato	407
Modalità di generazione dei report	415
Riferimenti per un modello di rapporto	416
Personalizzazione dei rapporti Crystal Reports	432

Capitolo 7: Inserimento dati in CA CMDB 433

Inserimento dati nel database	433
Modalità di inserimento dati nel database con GRLoader	433
Componenti di dati Federation Adapter	434
Input per Federation Adapters	434
Glossario di inserimento dei dati	435
Creazione di un nome fonte dati	435
Modalità di importazione dei dati mediante ADT	436
Aprire il Mapper ADT.	437
Impostazione della tabella di input	438
Impostazione del file di dati di destinazione	439
Impostazione di profili mediante Script Manager	440
Generazione dello script	441
Avvio del server ADT ed esecuzione dello script	441
Utilizzare iGRLoader per importare i dati	442
Federation Adapters	443
Prerequisiti per l'esecuzione di un Federation Adapter	443
Elenco di controllo dei Federation Adapter di CA Service Desk Manager	444
Assegnazioni classi e famiglie	445
Mapping dei dati fonte	446
Caricamento di elementi della configurazione da un foglio di calcolo Excel	446
Caricamento di server hardware da un foglio di calcolo Excel	447
Caricamento di relazioni da un foglio di calcolo Excel	448
Modalità di caricamento dei dati SMS Microsoft	448
Modalità di caricamento dei dati CA APM	449
Modalità di utilizzo del modello generico	450
Federation Adapter personalizzati	451

Capitolo 8: Utilizzo di MDR Launcher **453**

MDR Launcher	454
Terminologia MDR	455
Mapping di MDR	457
Avvio di MDR	457
Visualizzatore CMDBf	458
Definizione di un MDR per CA CMDB	458
Definizioni URL MDR	463
URL di avvio dell'MDR	464
Parametri per la sostituzione di URL	466
Federazione mediante GRLoader	468
Federazione di un elemento di configurazione	468
Definizione di più MDR in un elemento della configurazione mediante GRLoader	470
Associazione tra elementi della configurazione MDR ed elementi della configurazione di CA CMDB ..	471
Modalità di configurazione di MDR per visualizzatore CMDBf	473
Avvio dell'interfaccia del browser Web di MDR.	473
Integrazione di CA Cohesion	474

Capitolo 9: Gestione dei servizi Web **475**

Gestione dei servizi Web	475
Componenti di CA Service Desk Manager	476
Suggerimenti per i client dei servizi Web	476
Client Java	477
Configurazione dei servizi Web	479
Ridistribuzione dei servizi Web	480
Sicurezza dei servizi Web	481
Gestione degli errori	483
Errori di blocco	484
TimeOut	485
Codici di errore	485
Installazione dei servizi Web	487
Modalità di attivazione di Design-Time	487
Specifiche esterne	487
Autenticazione per l'accesso utente	488
Autenticazione Nome utente/Password	488
Autenticazione PKI (Public Key Infrastructure, infrastruttura a chiave pubblica)	490
Sessione e autorizzazione	495
Gestione e controllo dell'accesso	497
Oggetti	508
Aggiornamenti del sistema (cache)	509
Categorie e proprietà	510

Restituzione degli oggetti in formato XML	511
ITIL, metodologia	514
Creazione di incidenti o problemi	514
Query per incidenti o problemi	515
Associazione di un incidente a un problema	515
Associazione di un problema a un ordine di cambiamento	516
Elementi di configurazione	516
Utilizzo dei servizi Web	516
Accessi	516
Modalità di esecuzione di attività comuni	517

Capitolo 10: Integrazione con altri prodotti **521**

Integrazione di CA Workflow	521
Componenti di CA Workflow	522
Accesso CA Workflow	524
Integrazione di CA NSM	526
Modalità di integrazione con CA NSM	527
Configurare il convertitore in UNIX	528
Processo di post-integrazione	529
CA Service Desk Manager Event Converter	563
Potenziamento del processo di integrazione di NSM a CA Service Desk Manager	564
Integrazione di Portale CA	571
Verifica dell'accessibilità dell'interfaccia Web di CA Service Desk Manager	572
Installazione e avvio di Portale CA	572
Configurazione di CA Service Desk Manager per l'utilizzo di SSL con Portale CA	574
Integrazione di prodotti Mainframe	578
Caricamento dati lato CA Service Desk Manager	579
Prodotti CA che utilizzano CAISDI	579
Pianificazione dei prodotti CA per l'uso di CAISDI	580
Integrazione di CA Service Desk Manager con SAP Solution Manager	582
Prerequisiti per l'integrazione	582
Scenari di integrazione	584
Modalità di integrazione con SAP Solution Manager	587
Modalità di installazione di CASD Connector	588
Business Configuration Set	591
Modalità di configurazione di SAP Solution Manager	593
Modalità di configurazione di CA Service Desk Manager	602
Modalità di test dell'integrazione	604
Creazione di un ticket CA Service Desk Manager in SAP Solution Manager	607
Come tenere traccia degli incidenti SAP in CA Service Desk Manager	607
Creazione di un ticket CA Service Desk Manager che viene propagato a SAP Solution Manager	608
Visualizzazione di una richiesta CA Service Desk Manager	609

Visualizzazione del registro applicazione di sistema.....	610
Mantenimento dei dati di tabella in SAP Solution Manager	611
Messaggi definiti dall'integrazione con CA.....	611
Codici di eccezione restituiti da SAP Solution Manager a CA Service Desk Manager	613
Appendice A: Directory degli esempi	615
Contenuto della directory degli esempi	615
asset.....	615
Modalità di modifica del catalogo dei messaggi.....	615
macro_lock.....	616
ntf_meth	616
pdmconf	616
call_mgt	617
sdk	618
Appendice B: Caricamento di contenuti aggiuntivi	621
sd_content.dat	621

Capitolo 1: Introduzione

Questa sezione contiene i seguenti argomenti:

[Panoramica](#) (a pagina 15)

[Destinatari](#) (a pagina 15)

[Elenco utenti predefiniti di CA Service Desk Manager](#) (a pagina 16)

[Componenti server primari o secondari](#) (a pagina 17)

Panoramica

In questa guida vengono fornite le informazioni necessarie per una corretta implementazione di CA Service Desk Manager nella propria azienda. Sono incluse informazioni sulle procedure richieste per effettuare le operazioni seguenti:

- Pianificare e preparare una nuova installazione e un aggiornamento
- Installare e aggiornare tutti i componenti del prodotto necessari
- Configurare i componenti del prodotto
- Effettuare l'integrazione con alcuni prodotti CA

Nota: questa guida *non* specifica nei dettagli le integrazioni con tutti i prodotti CA. Per informazioni dettagliate su integrazioni aggiuntive con CA Service Desk Manager non descritte in questa guida, vedere il CA *Unicenter Service Desk Integrations Green Book* all'indirizzo <http://ca.com/support>.

Nota: è possibile reperire la versione più aggiornata delle Note di rilascio, contenente i requisiti di sistema e il file Leggimi facoltativo (se disponibile), all'indirizzo <http://ca.com/support>.

Destinatari

Questa guida è destinata a tutti coloro che desiderano informazioni su come installare, aggiornare e configurare CA Service Desk Manager. I seguenti utenti potrebbero dover completare attività specifiche utilizzando le informazioni fornite in questa guida:

- Gli *amministratori di sistema* e gli *amministratori* utilizzano le informazioni fornite in questa guida, insieme alle proprie conoscenze relative al sistema operativo, per installare il prodotto, aggiornarlo da una versione ad un'altra e configurarlo in base ai requisiti di implementazione.

- Gli *integratori* utilizzano le informazioni contenute in questa guida e le proprie conoscenze relative ai prodotti CA per integrare correttamente CA Service Desk Manager con alcuni prodotti CA.

Nota: questa guida *non* specifica nei dettagli le integrazioni con tutti i prodotti CA. Per informazioni dettagliate su integrazioni aggiuntive con CA Service Desk Manager non descritte in questa guida, vedere il CA *Unicenter Service Desk Integrations Green Book* all'indirizzo <http://ca.com/support>.

- Gli *utenti*, se necessario, possono utilizzare le informazioni contenute in questa guida per installare il prodotto e i componenti.

Per utilizzare le informazioni contenute in questa guida, è necessario:

- Avere conoscenza pratica dei sistemi operativi Windows e/o UNIX, in base all'ambiente di produzione corrente.
- Sapere eseguire attività amministrative di base per il sistema operativo in uso.
- A seconda dell'ambiente di lavoro, potrebbe inoltre essere necessario avere familiarità con il mainframe, i dispositivi mobili e le installazioni server.

Nota: all'interno di questa guida compaiono riferimenti a NX_ROOT. I riferimenti appartengono alla variabile di ambiente che contiene il percorso di installazione di CA Service Desk Manager. La variabile NX_ROOT viene impostata nel file di configurazione NX.env, in cui vengono definite le variabili di ambiente per CA Service Desk Manager.

Esempio definizione NX_ROOT

@NX_ROOT = C:\Program Files\CA\Service Desk Manager

Elenco utenti predefiniti di CA Service Desk Manager

Di seguito viene riportato un elenco delle informazioni relative agli utenti predefiniti per le implementazioni tipiche di CA Service Desk Manager:

Sistema operativo	Prodotto	Nome utente predefinito	Livello OS	Come viene creato
Windows	CA Service Desk Manager	ServiceDesk	Sì	Automaticamente
	CA Service Desk Manager	rhuser	Sì	Automaticamente
	FAST ESP	fastuser	Sì	Membro del gruppo amministrativo che dispone di una protezione speciale per l'accesso come servizio

Sistema operativo	Prodotto	Nome utente predefinito	Livello OS	Come viene creato
				creato automaticamente Non è un utente di dominio
	CA EEM	EiamAdmin		Password predefinita: EiamAdmin
	CA MDB SQL Server	ServiceDesk	No	Creato in MDB durante la configurazione
	CA MDB Oracle	mdbadmin	No	Creato in MDB durante la configurazione
UNIX	CA Service Desk Manager	srvcdesk	Sì	Creato manualmente
	FAST ESP	fastuser	Sì	Creato manualmente
	CA MDB Oracle	mdbadmin	No	Creato in MDB durante la configurazione

Componenti server primari o secondari

CA Service Desk Manager include componenti che si integrano tra loro e vengono eseguiti sul server *primario* o *secondario*. Prima di iniziare l'implementazione, è consigliabile acquisire alcune nozioni di base sui componenti seguenti:

Componenti server primari

I componenti seguenti vengono eseguiti su un server primario:

Gestione daemon (pdm_d_mgr)

Avvia i set di processi definiti nel file di avvio, ovvero pdm_startup.tpl. Per impostazione predefinita, la gestione dei daemon tenta l'avvio di un componente in cui si è verificato un errore per un massimo di 10 volte. Per verificare lo stato di tutti i componenti CA Service Desk Manager, utilizzare l'utilità pdm_status. L'utilità pdm_d_refresh consente di istruire la gestione dei daemon per l'avvio di un nuovo ciclo di 10 tentativi per processi contrassegnati come precedentemente non riusciti o in cui si è verificato un errore.

Message Dispatcher (sslump_nxd)

Funge da bus comune o sistema di passaggio dei messaggi. Per comunicare reciprocamente, i componenti devono prima registrarsi con Message Dispatcher. Quando un componente invia un messaggio, Message Dispatcher lo consegna ai componenti registrati per ricevere quel tipo di messaggio. Se due componenti comunicano in modo così frequente da rendere inefficace il passaggio dei messaggi attraverso Message Dispatcher, creano un canale rapido di comunicazione reciproca. È possibile visualizzare un elenco dei componenti registrati mediante l'utilità *s/stat*.

Agente di database (platform_agent)

Esegue query SQL sul database. Gli agenti di database si conformano allo schema logico di CA Service Desk Manager e convertono le istruzioni SQL di questo livello in istruzioni SQL della piattaforma del database fisico.

Nota: l'agente di database rileva la disconnessione temporanea e le query non riuscite e tenta la riconnessione e la comunicazione con il database. Ciò vale solo per i disservizi brevi, quali una breve interruzione di rete e una disconnessione temporanea. Non vale invece per i disservizi duraturi come la chiusura di un servizio di database per manutenzione e così via. L'agente tenta la connessione per un numero specificato di volte (l'impostazione predefinita è di tre volte) e solo per un periodo di tempo breve pari a pochi minuti. Se il disservizio dura di più, l'agente interrompe il tentativo di connessione ed è necessario riavviare CA Service Desk Manager una volta diventato di nuovo disponibile il database.

Provider agenti (platform_prov_nxd)

Avvia o arresta gli agenti di database. Per impostazione predefinita sono in esecuzione diversi agenti. Se ne sono richiesti altri per la gestione del numero di query del database, essi vengono avviati dal provider agenti. Se il sistema non richiede più un numero elevato di agenti di database, il provider agenti termina quelli non necessari.

Database virtuale (bpvirtdb_srvr)

Consente il funzionamento di più Gestioni oggetti. Tutte le Gestioni oggetti eseguite nel server primario o secondario si connettono al database virtuale, che ne arbitra l'accesso agli agenti di database. Quando viene ad esempio recuperato un nuovo intervallo di numeri di riferimento di ticket, il database virtuale garantisce che solo una Gestione oggetti alla volta acceda alla tabella contenente i numeri di riferimento. Il database virtuale esegue inoltre la memorizzazione nella cache delle informazioni del database per le Gestioni oggetti.

Archiviazione ed eliminazione continue (arcpur_srvr)

Esegue regole archiviazione ed eliminazione in base alla configurazione dell'amministratore CA Service Desk Manager.

Monitoraggio database (dbmonitor_nxd)

Esegue il monitoraggio dei cambiamenti a tabelle comuni in CA MDB, ad esempio *ca_contact*.

Daemon KPI (kpi_daemon)

Gestisce il recupero, l'organizzazione e l'archiviazione di dati relativi alla metrica dei KPI (Indicatori delle prestazioni chiave, Key Performance Indicator). Viene eseguito continuamente. Quando viene raggiunto il tempo di aggiornamento specificato di una query KPI, il daemon KPI interagisce con gli altri componenti di sistema per raccogliere i dati, quindi memorizza le metriche risultanti nel database.

License Manager (license_nxd)

Gestisce le licenze di CA per il prodotto.

Mail Daemon (pdm_mail_nxd)

Invia le notifiche di posta elettronica in uscita.

Mail Eater (pdm_maileater_nxd)

Accetta la posta elettronica in arrivo per gli aggiornamenti e la creazione di ticket.

Gestione notifiche (bpnotify_nxd)

Gestisce le notifiche in un ambiente Windows.

Controllo ortografia (lexagent_nxd)

Esegue il controllo ortografia come richiesto dai client.

Daemon Text API (pdm_text_nxd)

Crea e aggiorna i ticket tramite interfacce esterne, come la riga di comando o la posta elettronica.

Evento programmato (animator_nxd)

Specifica i tempi di ritardo degli eventi. In un'implementazione con molti tipi di servizio o contratti di assistenza, è possibile che il motore evento programmato debba tenere traccia di numerosi eventi attivi. In questa situazione, è necessario dedicare completamente Gestione oggetti del server primario al motore evento programmato. È possibile configurare altre Gestione oggetti sui server primario e secondario per l'accesso ai prodotti in base alle esigenze.

Ora violazione (ttv_nxd)

Calcola l'ora di violazione prevista per i tipi di servizio.

Componenti server primari o secondari

I componenti seguenti vengono eseguiti su un server primario o secondario:

Daemon Proctor (*pdm_proctor_nxd*)

Consente di avviare e riavviare componenti CA Service Desk Manager, come da istruzioni della Gestione daemon, su server primari e secondari. Quando si installa un server secondario, il processo *pdm_proctor_nxd* viene installato come servizio CA Service Desk Manager Remote Daemon Proctor. Quando viene avviato il server primario, Gestione daemon istruisce Remote Daemon Proctor per la connessione a Message Dispatcher. Gestione daemon istruisce quindi Remote Daemon Proctor per l'avvio dei componenti nel server secondario, come definito dai set di processi nel file di avvio *pdm_startup.tpl*.

Gestione oggetti (*domsrvr*)

Funge da processo server di CA Service Desk Manager. Quando si installa un server primario, per impostazione predefinita vengono installati due Gestioni oggetti, una per le connessioni al prodotto, l'altra dedicata a Screen Painter Web. Ciò consente di verificare le modifiche senza influenzare l'ambiente di produzione. Quando si installa un server secondario, è possibile configurare ulteriori Gestioni oggetti.

È necessario che una Gestione oggetti predefinita sia sempre in esecuzione nel server primario a cui client come il motore evento programmato possono connettersi.

Gestione oggetti memorizza inoltre nella cache vari record e tabelle per i client. Se si utilizza *pdm_userload* per manipolare tali record, è anche possibile utilizzare l'utilità *pdm_cache_refresh* affinché Gestione oggetti recuperi i nuovi dati.

Method Engine (*spel_srvr*)

Esegue codice, eventi, macro SPEL e così via per una Gestione oggetti. Si consiglia di eseguire ciascuna Gestione oggetti con il proprio method engine.

Server di accesso (*boplogin*)

Esegue la validazione dell'account utente del sistema operativo e le ricerche dei record contatto utilizzando il campo Accesso di sistema per trovare un utente con un determinato tipo di accesso.

Se l'azienda fornisce CA Service Desk Manager ad altre aziende client, è possibile inserire il server di accesso in un server secondario nella posizione di un singolo client. È quindi possibile abilitare l'autenticazione esterna nei tipi di accesso. Ciò evita la creazione di account utente per i client non inclusi nei sistemi aziendali.

Database virtuale LDAP (ldap_virtldb)

Si interfaccia con una directory LDAP.

Daemon Gestione delle informazioni (bpebr_nxd)

Esegue ricerche nella knowledge base. Al momento dell'avvio di CA Service Desk Manager il daemon bpebr_nxd memorizza nella cache i dati dei documenti della conoscenza dal database. Con una base documenti di grandi dimensioni è possibile che si verifichino problemi di risorse della memoria. Il daemon bpebr_nxd presenta i seguenti requisiti in termini di dimensioni:

Ricerca Gestione delle informazioni

- 100.000 documenti
- Dimensioni della memoria= 332.000 KB

Ricerca FAST ESP

- 2.000.000 documenti
- Dimensioni della memoria= 6.640.000 KB

Daemon di indicizzazione ricerca parole chiave/Gestione delle informazioni (bdeid_nxd)

Indicizza la knowledge base.

Daemon di classificazione FAQ Gestione delle informazioni (bu_daemon)

Calcola le classificazioni FAQ per Gestione delle informazioni.

Daemon della scheda Report della conoscenza (krc_daemon)

Esegue i calcoli per la funzione Scheda report della conoscenza Gestione delle informazioni. Questa funzione consente ad analisti e manager di visualizzare diverse viste matrice dei propri contributi alla conoscenza e di fornire feedback in cui siano evidenziati i documenti di maggiore efficacia. Le informazioni fornite possono essere utilizzate in vari modi per migliorare i processi di creazione dei documenti di conoscenza e fornire ai clienti la migliore assistenza.

Daemon Gestione delle informazioni(kt_daemon)

Gestisce la logica di gestione della conoscenza e di amministrazione della knowledge base, nonché il processo di approvazione dei documenti e le notifiche.

Supporto per siti multipli (pdm_global_nxd)

Esegue la replica tra una regione e la regione principale.

Repository Daemon (rep_daemon)

Gestisce i repository di allegati per CA Service Desk Manager e il daemon di ricerca parole chiave/Gestione delle informazioni.

Daemon controllo versioni (*pdm_ver_nxd*)

Sincronizza i file di schema tra un server primario e un server secondario per garantire che venga utilizzato lo stesso schema.

Server Web Apache Tomcat (*javaw*)

Consente l'implementazione di determinate funzioni, indipendentemente dall'utilizzo di Microsoft Internet Information Server (IIS) come server Web per l'accesso a CA Service Desk Manager. Tra queste funzioni sono inclusi CA Workflow, Elementi grafici, Allegati e Servizi Web.

Il server Web Apache Tomcat può essere amministrato tramite il controller Apache Tomcat (*pdm_tomcat_nxd*).

Web Engine (*webengine*)

Si connette ai browser Web attraverso un'interfaccia *pdmweb.cgi* in esecuzione in un server Web Microsoft IIS o Apache Tomcat. È necessario un motore Web per WSP sul server primario affinché la funzionalità di Progettazione schema WSP possa scrivere i file dello schema. I motori Web sono i client effettivi di una Gestione oggetti utilizzati dai browser Web per accedere al prodotto.

Moduli Web .html della cache dei motori Web per utenti connessi. È possibile modificare la cache utilizzando l'utilità *pdm_webcache* e visualizzare le statistiche relative alle connessioni utilizzando l'utilità *pdm_webstat*.

Capitolo 2: Aggiornamento

Questa sezione contiene i seguenti argomenti:

[Pianificazione dell'aggiornamento](#) (a pagina 23)

[Funzionamento della console di migrazione](#) (a pagina 35)

[Modalità di aggiornamento di CA CMDB da una versione precedente](#) (a pagina 37)

[Migrazione di dati Automazione supporto](#) (a pagina 40)

[Modalità di migrazione di un universo CA Business Intelligence personalizzato](#) (a pagina 45)

[Configurazione post aggiornamento](#) (a pagina 47)

Pianificazione dell'aggiornamento

È possibile aggiornare direttamente a CA Service Desk Manager r12.5 solo dalle versioni r11.2, r12.0 e r12.1.

Se si dispone di una versione precedente del prodotto, ad esempio Unicenter Service Desk r6.0 oppure r11.1, è *necessario* eseguire l'aggiornamento a CA Service Desk Manager r11.2 prima di eseguire l'aggiornamento a r12.5.

Importante CA Service Desk Manager supporta solo ITIL. Se si esegue l'aggiornamento da un sistema non ITIL, l'installazione di CA Service Desk Manager r12.5 effettua l'aggiornamento ad un ambiente ITIL.

Nota: per ulteriori informazioni sull'aggiornamento da una versione precedente, consultare la *versione r11.2 della Guida all'implementazione CA Service Desk Manager*. Per le patch di aggiornamento e assistenza tecnica, contattare il Supporto tecnico sul sito Web <http://ca.com/support>.

Importante Nel caso di installazione combinata di CA Service Desk Manager r11.2 e CA CMDB r11.1 non è possibile effettuare l'aggiornamento diretto a CA Service Desk Manager r12.5. È necessario *prima* aggiornare CA CMDB alla versione r11.2, quindi procedere con l'aggiornamento r12.5. CA Service Desk Manager verrà aggiornato dalla versione r11.2 alla versione r12.5 e CA CMDB verrà aggiornato dalla versione r11.2 alla versione r12.5. CA CMDB r12.0 può inoltre essere aggiornato direttamente a CA Service Desk Manager r12.5.

Prima di effettuare l'aggiornamento alla versione corrente di CA Service Desk Manager, è necessario leggere gli argomenti seguenti:

- [Considerazioni sui database](#) (a pagina 24)
- [Mantenimento delle personalizzazioni](#) (a pagina 27)
- [Considerazioni sulla migrazione LREL](#) (a pagina 30)
- [Considerazioni sulle transizioni di stato](#) (a pagina 32)
- [Considerazioni sulla posta elettronica](#) (a pagina 32)
- È necessario configurare le impostazioni internazionali UTF-8 sulle piattaforme Linux e UNIX.

Importante in ambienti Linux/UNIX, CA Service Desk Manager non utilizza più lo script `smtp_mail` per l'elaborazione delle notifiche di posta in uscita. Se l'utente che effettua l'aggiornamento alla versione corrente è un cliente esistente che utilizza `smtp_mail`, l'amministratore deve configurare opzioni di posta appropriate utilizzando la pagina relativa ai dettagli dei messaggi di posta elettronica predefiniti per abilitare la funzione di notifica di posta di CA Service Desk Manager.

Considerazioni sui database

Prima di eseguire l'aggiornamento a CA Service Desk Manager r12.5, tenere presenti le informazioni seguenti sui database:

- Eseguire una copia di backup del database esistente seguendo le procedure comunemente utilizzate per lo svolgimento di questo tipo di operazione.
- Archiviare la directory di installazione (`$NX_ROOT`) seguendo le procedure comunemente utilizzate per lo svolgimento di questo tipo di operazione. Questa operazione riduce il numero di trasferimenti dei dati risparmiando spazio su disco.
- Eseguire lo script appropriato per identificare eventuali record duplicati nel database:
 - (Oracle) Eseguire *OracleCheckr12UniqueIndexes.sql*, che si trova nella directory `\Migrate` del supporto di installazione.
 - (SQL Server) Aprire una finestra del prompt dei comandi ed eseguire *SQLCheckr12UniqueIndexes.sql* come segue:

```
cd $NX_ROOT\samples\views\SQLServer
```

Immettere il comando:

```
Sqlcmd -E -e < SQLServer\SQLCheckr12UniqueIndexes.sql
```


Nota: dopo avere eseguito l'aggiornamento a CA Service Desk Manager r12.5, questi file si trovano nel server in
`$NX_ROOT/samples/views/SQLServer` o
`$NX_ROOT/samples/views/Oracle`.

Importante tali script identificano i record duplicati. Eliminare i record duplicati identificati prima di procedere con la migrazione.

- Aggiornare il sistema CA Service Desk Manager r11.2 ad un database supportato (SQL Server e Oracle).

Nota: per ulteriori informazioni sul database supportato, vedere le *Note di rilascio*.

- Eseguire l'aggiornamento da Unicenter Service Desk r11.0 a CA Service Desk Manager r11.2 prima di eseguire la migrazione dei dati in un database supportato.
- Se si immettono caratteri Windows speciali, ad esempio un trattino lungo, in CA Service Desk Manager o Gestione delle informazioni o in un sistema non Windows, tali caratteri non verranno archiviati in maniera corretta nel database.
- **Ingres** - Se si utilizza un database Ingres, convertire i dati in Oracle o SQL Server prima di eseguire l'aggiornamento.

Nota: per informazioni sul processo di conversione, consultare la documentazione relativa al database.

- **Oracle** - Oracle non supporta l'uso indistinto di maiuscole e minuscole negli indici per la registrazione degli elementi della configurazione. Prima di avviare la migrazione in Oracle, verificare che SQLPlus e Oracle DB siano in grado di comunicare utilizzando il nome host. Se si verifica un errore di comunicazione, verificare che Oracle sia configurato con un adattatore di loopback.
- **SQL Server** - Se si utilizza SQL Server e si effettua l'aggiornamento alla versione corrente di CA Service Desk Manager, il database predefinito per l'ID utente database configurato deve essere CA MDB. Se il database predefinito non è CA MDB, la console di migrazione non funziona correttamente e viene visualizzato il messaggio seguente:
"La tabella acctyp_v2 non esiste sull'MDB"
- **Tomcat** - Se Tomcat è stato configurato per l'autenticazione esterna con Unicenter Service Desk r11.0, r11.1 o CA Service Desk Manager r11.2, è *necessario* riconfigurare manualmente Tomcat per l'autenticazione esterna dopo l'aggiornamento alla versione corrente del prodotto.

- **Aggiornamenti tabelle** - Tenere presenti gli aggiornamenti delle tabelle seguenti che si verificano durante la migrazione:
 - **Tabelle di stato** - Queste tabelle vengono aggiornate anche con i record di stato appropriati se nel database non esistono gli stessi valori di codice. La tabella *Cr_Status*, ad esempio, viene aggiornata con il codice *AEUR* (Awaiting End User Response).
 - **Aree funzionali** - Per ciascun ruolo, la migrazione aggiunge automaticamente una riga per ogni record *usp_functional_access*. Durante la migrazione, il livello di accesso è impostato sullo stesso valore per ciascuna area funzionale di CA Service Desk Manager r12.0 e r12.1 che si trova nella tabella *usp_role*. Le nuove aree funzionali vengono mappate utilizzando un campo di riferimento.
- **Chiavi esterne** - Tenere presenti le informazioni seguenti:
 - Le chiavi esterne (SREL) che fanno riferimento a tabelle la cui chiave primaria è un UUID vengono cambiate dal tipo a numero intero al tipo UUID (o a 16 byte).

Nota: per informazioni sull'impostazione degli attributi SREL con i valori chiave esterna, consultare la *Guida di riferimento tecnico di CA Service Desk Manager*.
 - Se nel sistema CA Service Desk Manager precedente sono stati rimossi i vincoli delle chiavi esterne per il caricamento di massa dei dati, è necessario ricordarsi di creare nuovamente tali vincoli prima di eseguire l'aggiornamento. Gli script che rimuovono i vincoli si trovano nei percorsi seguenti:
 - Oracle
\$NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql
 - SQL Server
\$NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql

Nota: applicare nuovamente i vincoli rimossi mediante l'esecuzione degli script appropriati *OracleAddConstraints.sql* oppure *SQLServer/SQLAddConstraints.sql*. Tali script si trovano nella stessa directory dei vincoli rimossi, con le istruzioni incluse nei file menzionati.

- **MDB** - Fornisce uno schema di database coerente per diversi dati di gestione IT. Durante lo sviluppo dell'MDB, gli elementi dati dell'ambiente CA Service Desk Manager precedente sono incorporati in questo schema. Le dimensioni degli elementi di dati possono aumentare e, di conseguenza, aumenta anche la dimensione complessiva del database.

Nota: se le dimensioni degli elementi dati standard superano la larghezza delle colonne definita per l'MDB, è possibile che i dati vengano troncati durante il processo di aggiornamento. In questo caso, vengono visualizzati dei messaggi di notifica.

- **Configurazione distribuita** - È consigliabile aggiornare il server primario prima di qualsiasi server secondario.
- **Configurazione dei database remoti** - Tenere presenti le informazioni seguenti:
 - È consigliabile aggiornare il server di database con un nuovo MDB prima di aggiornare il server primario. Se il server di database è remoto, eseguire l'installazione di CA MDB nel server di database prima di eseguire l'aggiornamento.
 - Se si utilizza un database MDB SQL Server, è necessario che sqlcmd si trovi nel computer client prima di eseguire la connessione all'MDB remoto.

Mantenimento delle personalizzazioni

Prima di effettuare l'aggiornamento a CA Service Desk Manager r12.5, tenere presenti le informazioni seguenti se il prodotto è stato personalizzato.

Nota: chiudendo la console di migrazione prima del completamento dell'aggiornamento, il processo continuerà ad essere eseguito in background.

- **Report personalizzati** - Se sono stati personalizzati i report che consentono di accedere a tabelle di database di versioni precedenti che sono stati spostati in tabelle rinominate, i nomi delle colonne in r12.5 sono cambiati.

Nota: per informazioni sulle tabelle, consultare la *Guida di riferimento tecnico di CA Service Desk Manager*.

- **Moduli personalizzati** - L'aggiornamento alla versione corrente di CA Service Desk Manager consente di conservare le personalizzazioni dei moduli della versione precedente. È tuttavia possibile che non si riesca a visualizzare le funzionalità di r12.5 nei moduli personalizzati aggiornati.

- **Struttura Amministrazione personalizzata** - Se la Struttura Amministrazione è stata personalizzata in Unicenter Service Desk r11.0, i cambiamenti non vengono aggiornati a causa delle modifiche apportate nell'architettura per il supporto dell'interfaccia utente basata su ruoli. In queste personalizzazioni della Struttura Amministrazione è inclusa l'aggiunta di nuovi nodi, la ridenominazione di nodi esistenti e la modifica di tipi di accesso o di altre alterazioni di dati. È possibile continuare ad utilizzare le personalizzazioni seguendo le indicazioni seguenti:
 1. Prima di eseguire l'aggiornamento, rivedere la Struttura Amministrazione di Unicenter Service Desk r11.0 e prendere nota di eventuali personalizzazioni che si desidera mantenere dopo l'aggiornamento.
 2. Al termine dell'aggiornamento, identificare i ruoli che presentano le personalizzazioni della Struttura Amministrazione.
 3. Applicare le personalizzazioni alle Strutture Amministrazione basate su ruoli di CA Service Desk Manager r12.5 appropriate.
 4. Rivedere e verificare che la funzionalità desiderata sia stata mantenuta.

- **Pulsanti dei moduli personalizzati** - Dopo l'aggiornamento, i pulsanti nei moduli personalizzati in `/site/mods/html` la cui parte di codice msgtxt (n) non è racchiusa tra virgolette restituiscono un messaggio di errore invece del nome del pulsante.

Ad esempio, nel modulo `detail_cr.html`, modificare `msgtxt(441)` racchiudendolo tra virgolette per visualizzare il nome di pulsante corretto:
`ImgBtnCreate (" btnchg", "msgtxt(441)", "detailSave ('NEW_CHANGE')",
true, 0, msgtxt(440)); // Salva e Crea ordine di cambiamento`

- **Conservazione delle personalizzazioni** - Se è necessario disporre della funzionalità CA Service Desk Manager r12.5 e si desidera conservare le personalizzazioni, è necessario ripetere tali personalizzazioni sulla base del modulo CA Service Desk Manager r12.5 in cui sono disponibili le nuove funzioni di r12.5.

Nota: se i report `acctypedtl.rpt` e `acctypesum.rpt` sono stati personalizzati, i dati restituiti da CA Service Desk Manager r12.5 saranno obsoleti.

- **Regole di notifica** - Se dalla precedente installazione di CA Service Desk Manager sono state rimosse le notifiche delle attività predefinite Contatto, Contatti oggetto e Tipi contatto e si desidera invece mantenere tali funzioni, prendere nota dei contatti predefiniti rimossi prima della migrazione. Una volta effettuato l'aggiornamento alla nuova versione, rimuovere nuovamente i contatti Notifica predefiniti.

- **Funzionalità basata sui ruoli** - L'aggiornamento può determinare problemi con la funzionalità basata sui ruoli. Prendere in considerazione le informazioni seguenti:
 - Se i seguenti moduli sono stati personalizzati, vengono considerati di sola lettura dal Screen Painter Web in CA Service Desk Manager r12.5 e includono una versione xxx_site.html in cui è possibile utilizzare codice personalizzato:
 - ahdtop.html
 - menu_frames.html
 - reports.html
 - std_body.html
 - std_footer.html
 - std_head.html
 - styles.html
 - msg_cat.js
 - menu_frames_role.html
 - **File HTML personalizzati** - Tutti i file HTML personalizzati mantengono le impostazioni predefinite della barra dei menu dopo l'aggiornamento. Una finestra popup eredita la barra dei menu dalla scheda della pagina principale in seguito alla creazione dell'interfaccia utente basata su ruoli e non sarà disponibile nei moduli personalizzati della versione precedente dopo l'aggiornamento.
 - Alcuni file HTML personalizzati delle versioni precedenti non vengono più utilizzati nella versione corrente. Effettuare le operazioni seguenti dopo l'aggiornamento:
 - a. Eseguire *pdm_perl \$NX_ROOT/bin/migrate_to_r12_5_web_check.pl* per aggiungere i file con un'estensione *incompatible_for_r12_5*.
 - b. Aprire *\$NX_ROOT/bin/migrate_to_r12_5_web_check.p* con un editor di testo per visualizzare un elenco di moduli non compatibili con la versione r12.5.
- **Chiavi esterne** - Se il processo di aggiornamento rileva problemi di integrità referenziale quando si prova a reimpostare le chiavi esterne, nel file migration.log vengono visualizzati errori. La chiave esterna associata viene impostata su un riferimento valido predefinito.

- **Configurazione di Web Director, server primario/secondario** - Se l'installazione precedente è stata configurata per l'utilizzo di server secondari Web Director, è *necessario* eseguire `$NX_ROOT\samples\pdmconf\pdm_edit.pl` dopo l'aggiornamento. Attenersi ai passaggi definiti in `pdm_edit.pl` per completare la configurazione.

Nota: i server secondari e i Web Director non funzionano se non si esegue `pdm_edit.pl` su un sistema aggiornato.
- **Divisioni di CA Automazione supporto** - Se si desidera [migrare le divisioni](#) (a pagina 41) in titolari, convertire questi dati prima di abilitare e configurare Automazione supporto in CA Service Desk Manager r12.5.

Considerazioni sulla migrazione LREL

Una *List Relationship* (LREL) rappresenta un'associazione tra due oggetti. La relazione può avere un lato sinistro (lhs) e un lato destro (rhs). Ogni lato della relazione è un attributo dell'oggetto majic contenente la relazione dati.

Nelle versioni precedenti del prodotto gli oggetti e le istruzioni LREL .maj descrivono relazioni dati DBMS multi-a-molti. Tali relazioni non utilizzano più l'istruzione majic LREL, in quanto entrambi i lati della relazione vengono archiviati in singole tabelle. Gli oggetti accedono alla relazione mediante un'istruzione BREL standard. È ad esempio possibile visualizzare la relazione tra ordini di cambiamento ed elementi di configurazione esaminando la nuova tabella `usp_lrel_asset_chgnr` e l'oggetto `lrel_asset_chgnr` corrispondente.

Grazie alle modifiche apportate a LREL non è più necessario archiviare i nomi degli attributi nel database. I due lati della relazione rappresentano singole relazioni di chiavi esterne (SREL) che possono essere unite e indicizzate facilmente. Se necessario, la relazione può contenere ulteriori attributi relazionali.

Durante l'aggiornamento, si verificano le attività seguenti mentre è in corso la migrazione dei dati della tabella LREL in r12.5:

- Le tabelle e gli oggetti con relazioni LREL vengono migrati automaticamente nelle tabelle e negli oggetti r12.5.
- Alle nuove tabelle viene assegnato un nome con il formato `usp_lrel_lhsName_rhsName`.

La tabella `usp_lrel_asset_chgnr` presenta ad esempio una relazione sul lato sinistro con gli asset e una relazione sul lato destro con gli ordini di cambiamento.

- Agli oggetti corrispondenti viene assegnato un nome nel formato *lrel_lhsName_rhsName*.

L'oggetto *lrel_asset_chgnr* corrisponde ad esempio alla tabella *usp_lrel_asset_chgnr*.

- A causa di una restrizione del database, alcuni nomi vengono abbreviati.
- I dati migrano dalle tabelle precedenti nelle tabelle r12.5 e tutto il codice CA Service Desk Manager viene modificato per l'utilizzo di queste tabelle.
- Nel sistema non vengono più utilizzate le precedenti tabelle di database LREL, ad esempio *bmlrel*. A scopo di riferimento, tuttavia, nelle tabelle precedenti i dati vengono conservati.
- Un attributo Backward Relation (BREL) per il nuovo oggetto sostituisce l'attributo LREL originale in ogni definizione di oggetto majic correlata.
- Se si utilizza un'API supportata, ad esempio il metodo del servizio Web *CreateLrelRelationship()*, il codice funziona nel modo previsto.
- Se sono state aggiunte relazioni di tipo LREL personalizzate, vengono migrate da CA Service Desk Manager nelle tabelle r12.5.
- Il codice o i report definiti a livello di sito che accedono direttamente alle tabelle LREL precedenti agiscono sui dati precedenti in quanto nel sistema tali tabelle non vengono più utilizzate. È consigliabile aggiornare il codice per l'utilizzo delle tabelle r12.5 in modo da garantire la corretta esecuzione del codice e dei report.

Importante Se il codice accede direttamente agli oggetti o alle tabelle LREL precedenti restituisce un errore al termine della migrazione. È consigliabile aggiornare il codice prima della migrazione. Se, ad esempio, nel codice vengono utilizzate istruzioni majic per stabilire relazioni LREL, utilizzare il metodo *createLrelRelationships()* anziché compilare direttamente una tabella.

Nota: è consigliabile verificare il codice o i report definiti a livello di sito che accedono direttamente al database o che utilizzano gli oggetti majic LREL precedenti come l'oggetto *lrel1* per verificarne il corretto funzionamento. È possibile aggiornare il codice in modo da utilizzare un'interfaccia supportata, ad esempio Servizi Web. È inoltre necessario aggiornare i nomi di tabella. Per i report, è anche possibile aggiornare le query con i nuovi riferimenti di tabella DBMS.

Considerazioni sulle transizioni di stato

Se si intende utilizzare le transazioni di stato in seguito all'aggiornamento a CA Service Desk Manager r12.5, tenere presente le informazioni seguenti:

- Le transazioni di stato non sono attive quando si esegue l'aggiornamento a r12.5.

Nota: tutte le descrizioni di codice di stato personalizzate che compaiono in moduli di ticket vengono trattenute durante il processo di aggiornamento.

- L'opzione *Status_Policy_Violations* viene installata e impostata su Warn per impostazione predefinita dopo l'aggiornamento. Questa impostazione consente l'esecuzione di transizioni indefinite, ma registra un avviso.
- Se si imposta l'opzione su Allow, le transazioni indefinite non vengono registrate.

Nota: per ulteriori informazioni sull'opzione *Status_Policy_Violations*, vedere la *Guida in linea*.

Aggiornamento della posta elettronica

CA Service Desk Manager sostituisce le opzioni per la posta elettronica in arrivo di Gestione opzioni, Posta elettronica con una casella di posta (tabella *usp_mailbox*) che offre opzioni corrispondenti. Le opzioni per la posta elettronica in uscita di Posta elettronica sono ancora disponibili in Gestione opzioni. Quando si esegue l'aggiornamento, CA Service Desk Manager utilizza le impostazioni esistenti per la posta elettronica per configurare una casella di posta, anziché le impostazioni predefinite della casella di posta fornite con CA Service Desk Manager r12.5. Ogni opzione di posta elettronica, tranne EMAIL_ATTACHMENT_DIR che non è più necessaria, viene mappata a un'opzione nella tabella *usp_mailbox*. Le opzioni non impostate, vengono impostate come NULL nella tabella.

Nota: per informazioni sull'attivazione della casella di posta predefinita e sull'utilizzo delle opzioni della casella di posta, consultare la *Guida all'amministrazione* e la *Guida in linea*.

Nella tabella seguente sono elencate le opzioni rimosse da Posta elettronica e riportate nella tabella *usp_mailbox* e ne viene indicata l'etichetta nella pagina Dettagli casella di posta:

Opzione di posta elettronica	Opzione usp_mailbox	Etichetta dettagli casella di posta predefinita
EMAIL_ALLOW_ANONYMOUS	allow_anonymous	Consenti anonimo
EMAIL_ATTACHMENT_DIR	N/D	N/D

Opzione di posta elettronica	Opzione <i>usp_mailbox</i>	Etichetta dettagli casella di posta predefinita
		Nota: poiché l'opzione <code>EMAIL_ATTACHMENT_DIR</code> è obsoleta, è necessario selezionare manualmente un Repository allegati se questa opzione è stata impostata e l'opzione <code>EMAIL_ATTACHMENT_REPOSITORY</code> non è stata impostata.
<code>EMAIL_ATTACHMENT_REPOSITORY</code>	<code>attmnt_repository</code>	Repository allegati
<code>EMAIL_FORCE_ATTACHMENT_SPLITOUT</code>	<code>split_out_attachment</code>	Imponi separazione degli allegati
<code>EMAIL_IS_ATTACHMENT</code>	<code>attach_email</code>	Allega intero messaggio di posta elettronica
<code>EMAIL_SAVE_UNKNOWN_EMAILS</code>	<code>save_unknown_emails</code>	Salva messaggi di posta elettronica sconosciuti
<code>MAIL_EATER_IMAP_HOST_PORT</code>	<code>host_port</code>	Ignora porta
<code>MAILEATER_CHECK_MAIL_INTERVAL</code>	<code>check_interval</code>	Intervallo di controllo
<code>MAILEATER_HOST</code>	<code>host_name</code>	Nome host
<code>MAILEATER_LOGIN_PASSWORD</code>	<code>password</code>	Password
<code>MAILEATER_LOGIN_USERID</code>	<code>ID utente</code>	Userid
<code>MAILEATER_POP3_HOST_PORT</code>	<code>host_port</code>	Ignora porta
<code>MAILEATER_SECURITY_LEVEL</code>	<code>security_lvl</code>	Livello di protezione
<code>MAILEATER_SERVER_TYPE</code>	<code>email_type</code>	Tipo di messaggio di posta elettronica

Importante L'impostazione Directory allegati è obsoleta in r12.5, pertanto è *necessario* specificare un Repository allegati per poter continuare il polling delle caselle di posta.

Considerazioni su *Maileater.cfg*

Le informazioni incluse in precedenza nel file *maileater.cfg* vengono mappate alla tabella *usp_mailbox_rule* in r12.5. Considerare le informazioni seguenti sul mapping da *maileater.cfg* a *usp_mailbox_rule*:

- L'opzione "-i" all'inizio della riga denota la mancata applicazione della distinzione tra maiuscole e minuscole e consente di eseguire il mapping al campo `filter_ignore_case`.

- Il filtro di ricerca "Subject: *..." indicava in precedenza un'espressione regolare in base alla quale applicare il filtro. "Subject:" viene rimosso, sostituito da un simbolo "^" e il valore rimanente esegue il mapping al campo *filter_string*. *Filter_type* viene impostato sul tipo "Subject Contains".
- "TEXT_API xxx" indica l'oggetto elaborato per la regola. La stringa "TEXT_API" viene rimossa e la parte restante esegue il mapping al campo *action_object*. Il campo *action_operation* viene impostato su Crea/Aggiorna oggetto.
- La risposta all'utente contiene in genere "PDM_MAIL ...". Se "PDM_MAIL" è impostato, impostare *reply_method* su 1800 o lasciarlo impostato su null.
- Se il parametro *-s* è impostato, rimuovere il campo *subject* dal testo e impostare *reply_subject* su questo valore.
- La funzionalità mantiene l'ordine delle voci. Per ogni riga valida viene impostato un numero di sequenza che inizia da 100 e viene incrementato di 100.

Gli altri campi di *usp_mailbox_rule* vengono impostati nel modo seguente:

Campo	Valore
mailbox	Predefinito
action_write_to_log	0
action_log_prefix	null
delete_flag	0
descrizione	Migrato dal file <i>pdm_maileater.cfg</i>
reply_failure_html	<lasciare vuoto per ereditare l'azione predefinita>
reply_failure_text	<lasciare vuoto per ereditare l'azione predefinita>
reply_success_html	<lasciare vuoto per ereditare l'azione predefinita>
reply_success_text	<lasciare vuoto per ereditare l'azione predefinita>
text_api_defaults	null
text_api_ignore_incoming	null
action_subject_handling	null
last_mod_dt	null
last_mod_by	null

Campo	Valore
inclusion_list	"*"
email_address_per_hour	-1
exclusion_list	null
log_policy_violation	1

Funzionamento della console di migrazione

La console di migrazione guida l'utente nel processo di migrazione e aggiornamento per CA Service Desk Manager. La console rileva automaticamente un'installazione esistente, ad esempio CA Service Desk Manager r11.2. È possibile avviare l'aggiornamento dal supporto di installazione oppure [manualmente](#) (a pagina 36).

Importante La console di migrazione CA Service Desk Manager non converte le divisioni in titolari. Se si desidera configurare Automazione supporto in un ambiente multi-tenancy, è *necessario* [migrare separatamente](#) (a pagina 41) le divisioni di CA Automazione supporto r6.0 SR1 eFix5 in titolari r12.5 prima di abilitare Automazione supporto in CA Service Desk Manager.

La console effettua le operazioni seguenti:

1. Verifica che il prodotto sia CA Service Desk Manager r11.2, r12.0 o r12.1.
2. Converte le password in formato compatibile con FIPS 140-2.
3. Applica gli aggiornamenti MDB.

Importante La versione MDB remota deve essere almeno r1.5. In caso contrario, la migrazione non riesce.

4. Migra i dati LREL.
5. Converte i file personalizzati in UTF-8.
6. Converte i record relativi al tipo di accesso in record relativi al tipo di accesso e ruolo per CA Service Desk Manager r12.5.
7. Migra e aggiorna le query del contatore dell'utente per le operazioni basate sui ruoli.
8. Migra e aggiorna le notifiche esistenti per l'utilizzo delle regole di notifica e dei modelli dei messaggi di notifica.

Nota: dopo aver selezionato Esegui aggiornamento e fatto clic su Installa, non è possibile ripristinare la migrazione e l'aggiornamento. Nota: chiudendo la console di migrazione prima del completamento del processo, il processo continuerà ad essere eseguito in background.

Ulteriori informazioni:

[Installazione dell'CA MDB](#) (a pagina 116)

[Configurazione del prodotto](#) (a pagina 165)

[Modalità di aggiornamento di CA CMDB da una versione precedente](#) (a pagina 37)

[Migrazione di dati Automazione supporto](#) (a pagina 40)

File di registro della migrazione

Se si verificano problemi durante la migrazione e l'aggiornamento, il registro della migrazione fornisce un record dell'intero processo. Tale registro si trova nel percorso seguente:

`$NX_ROOT/log/pdm_migrationr12_5.log`

Avvio manuale della migrazione

È possibile avviare manualmente l'aggiornamento utilizzando il comando seguente:

■ Windows

`$NX_ROOT\bin\migrate_to_r12_5.vbs`

■ Linux/UNIX

`$NX_ROOT/bin/migrate_to_r12_5.sh`

Nota: se la migrazione non riesce e si verifica un errore di validazione dello schema, utilizzare il comando sopra menzionato per eseguire nuovamente l'aggiornamento.

Ulteriori informazioni:

[Considerazioni sui database](#) (a pagina 24)

[Mantenimento delle personalizzazioni](#) (a pagina 27)

[Considerazioni sulla migrazione LREL](#) (a pagina 30)

[Funzionamento della console di migrazione](#) (a pagina 35)

[File di registro della migrazione](#) (a pagina 36)

[Avvio manuale della migrazione](#) (a pagina 36)

Modalità di aggiornamento di CA CMDB da una versione precedente

È possibile aggiornare CA CMDB a CA Service Desk Manager r12.5 da una versione precedente, ad esempio r11.2 e r12.0. Se si annulla la migrazione, è *necessario* eseguire lo script per riavviare la console di migrazione. Lo script si trova nella directory */bin* del prodotto, ad esempio *C:/CMDB/bin*. Se, ad esempio, si annulla la migrazione in Linux o Unix, eseguire lo script *migration_to_r12.5.sh*.

Nota: se si esegue l'aggiornamento a una versione autonoma di CA CMDB, è possibile continuare a utilizzare le funzionalità autonome di CA CMDB in CA Service Desk Manager r12.5. Se si esegue l'aggiornamento da un ambiente con CA CMDB e CA Service Desk Manager o da un ambiente CA Service Desk Manager senza CA CMDB, la versione completa di CA Service Desk Manager r12.5 viene installata durante l'aggiornamento.

Per aggiornare CA CMDB, procedere nel modo seguente:

1. Avviare il programma di installazione di CA Service Desk Manager dal supporto di installazione.

Il programma di installazione rileva la versione del prodotto, ad esempio CA CMDB r11.2.

Nota: se si esegue l'aggiornamento da un'installazione combinata di CA Service Desk Manager e CA CMDB, il programma di installazione visualizza l'ambiente rilevato come versione di CA CMDB e non di CA Service Desk Manager.

2. Fare clic su Avanti.

Verrà visualizzato l'avviso di non utilizzare CA Service Desk Manager e Gestione delle informazioni finché la migrazione non sarà stata completata.

3. Fare clic su Avanti.

Se l'installazione rileva Visualizer, viene richiesto di disinstallarlo manualmente.

Importante Dopo aver disinstallato Visualizer, è *necessario* riavviare il programma di installazione di CA Service Desk Manager.

4. Accettare i termini del contratto di licenza, quindi fare clic su Installa.

Viene eseguito il backup dei dati dell'utente e i servizi vengono chiusi.

Nota: durante l'aggiornamento di CA CMDB *non* viene eseguito il backup del database.

Al termine dell'installazione, viene visualizzata la console di migrazione con l'avviso di consultare la documentazione relativa alla migrazione.

5. Fare clic su Esegui migrazione.

Nella console di migrazione vengono caricati i dati del sistema, viene aggiornato l'MDB e vengono riciclati i servizi.

Nota: durante il processo è possibile visualizzare attivamente il registro di migrazione.

6. Nella console vengono verificate le tabelle, elaborati i dati, nonché eseguiti il backup e l'aggiornamento del prodotto alla r12.5.

Viene visualizzata la configurazione di CA Service Desk Manager.

7. (Facoltativo) Configurazione solo CMDB.

Se si esegue l'aggiornamento da un ambiente CA CMDB autonomo, nel modulo Impostazioni generali viene visualizzata la casella di controllo *Configurazione solo CMDB*.

Importante Durante la configurazione, quando viene eseguita la migrazione dalla versione autonoma di CA CMDB a CA Service Desk Manager, viene visualizzata la casella di controllo Configurazione solo CMDB. Se si deseleziona la casella di controllo Configurazione solo CMDB e si fa clic su Avanti, non è più possibile configurare CA CMDB. Anche se si sceglie Indietro, la casella di controllo Configurazione solo CMDB non è più disponibile. Un messaggio informa l'utente di questo comportamento nella finestra di dialogo della configurazione. Se si annulla la configurazione prima del termine e la si riesegue, la casella di controllo Configurazione solo CMDB è nuovamente disponibile.

La casella di controllo Configurazione solo CMDB controlla il valore della variabile di ambiente NX_CMDB di CA Service Desk Manager. La variabile di ambiente controlla se è configurata la funzione Automazione supporto. Se la casella di controllo è deselezionata, Automazione supporto è configurabile; in caso contrario, non lo è. La variabile di ambiente influisce sul comportamento di alcuni moduli Web.

Se si esegue l'aggiornamento da un ambiente CA CMDB autonomo e si desidera utilizzare le funzionalità autonome di CA CMDB in CA Service Desk Manager r12.5, non è possibile configurare Automazione supporto.

8. Completare la configurazione nel modo appropriato all'ambiente corrente.

Migrazione di dati Automazione supporto

È possibile migrare dati CA Automazione supporto r6.0 SR1 eFix5 in CA Service Desk Manager r12.5 dagli ambienti seguenti:

- Unicenter Service Desk r11.2
- CA Service Desk Manager r12.0
- CA Service Desk Manager r12.1
- CA Automazione supporto r6.0 SR1 eFix5 senza CA Service Desk Manager.

Nota: è possibile migrare solo dati da CA Automazione supporto r6.0 SR1 eFix5. Prima di procedere alla migrazione, è consigliabile eseguire un backup completo del database di CA Automazione supporto r6.0 SR1 eFix5.

Importante Le personalizzazioni da CA Automazione supporto r6,0 SR1 eFix5 non migrano automaticamente a CA Service Desk Manager r12.5. Si consiglia di controllare la personalizzazione per verificare che corrisponda alla personalizzazione CA Service Desk Manager. Se necessario, copiare e incollare i dati relativi a intestazione, piè di pagina e URL CSS di ciascuna divisione nel titolare (o pubblico) corrispondente in CA Service Desk Manager per la migrazione dei dati di personalizzazione.

Modalità di migrazione di un database di Automazione supporto

È possibile configurare lo strumento di migrazione per migrare dati dal database di Automazione supporto nel database di CA Service Desk Manager, inclusa la trasformazione dei nomi Automazione supporto in base alle convenzioni del database di CA Service Desk Manager. Migrare i dati dal database di Automazione supporto nel database di CA Service Desk Manager prima di utilizzare Automazione supporto per la prima volta.

Nel processo seguente viene descritto come migrare i dati:

1. [Esportare](#) (a pagina 42) i dati CA Automazione supporto utilizzando lo script del supporto di installazione.

Lo strumento di esportazione converte i dati nel formato *.DAT*. Esegue inoltre i passaggi principali seguenti durante la migrazione dei dati:

- Importazione dello schema del database di Automazione supporto nel database di CA Service Desk Manager.

Questo schema crea le tabelle necessarie utilizzate da Automazione supporto.

- Migrazione dei dati dall'XML di migrazione del database di Automazione supporto nel database di CA Service Desk Manager.

Lo strumento di migrazione di CA Service Desk Manager genera gli UUID e i record necessari che rappresentano le relazioni tra l'ID di Automazione supporto e l'UUID di CA Service Desk Manager.

2. Copiare la cartella di esportazione dati Automazione supporto di CA nella directory seguente nel server CA Service Desk Manager:

NX_ROOT/site/sbmigration/SA60

Verrà completata l'esportazione dei dati.

3. [Importare](#) (a pagina 44) i dati in CA Service Desk Manager utilizzando lo strumento di migrazione Automazione supporto di CA.

I dati vengono caricati nel database e la migrazione verrà completata.

Migrazione di dati cronologici

Se non si desidera migrare tutti i dati cronologici dal database di CA Automazione supporto r6.0 SR1 eFix5, è possibile eliminarne solo alcuni. Durante l'impostazione dello script di eliminazione è possibile configurare il numero di giorni da conservare nel database.

Tale script può essere scaricato dall'indirizzo seguente:

ftp://ftp.ca.com/pub/supportbridge/6,0/patch-01/purge_history_6.0_sp1.zip

Modalità di conversione di divisioni in titolari

È possibile effettuare solo la migrazione di divisioni da CA Automazione supporto r6,0 SR1 eFix5. Tali divisioni vengono convertite in titolari per utilizzare la multi-tenancy in un ambiente Automazione supporto. È possibile migrare ogni divisione separatamente nel rispettivo titolare. Durante l'importazione iniziale dei dati, tutte le righe nelle tabelle con titolari facoltativi vengono occupate da titolari.

Importante La migrazione dei dati viene eseguita prima di abilitare Automazione supporto in CA Service Desk Manager.

È possibile migrare le divisioni nei titolari nel modo seguente:

1. [Esportare](#) (a pagina 42) i dati della divisione utilizzando lo script del supporto di installazione.

È possibile esportare una o tutte le divisioni.

2. Lo strumento di esportazione converte i dati nel formato *.DAT*.
Lo strumento visualizza lo stato di esportazione della divisione.

3. Copiare la cartella di esportazione dati Automazione supporto di CA nella directory seguente nel server CA Service Desk Manager:

`NX_ROOT/site/sbmigration/SA60`

Verrà completata l'esportazione dei dati.

4. [Importare](#) (a pagina 44) i dati in CA Service Desk Manager utilizzando lo strumento di migrazione Automazione supporto di CA.

I dati vengono caricati nel database e la migrazione verrà completata.

Nota: per ulteriori informazioni sulla configurazione di Automazione supporto, vedere la *Guida in linea*.

Esportazione di dati CA Automazione supporto

Per esportare i dati CA Automazione supporto r6.0 SR1 eFix5 è necessario convertirli nel formato `.DAT` utilizzato in CA Service Desk Manager. È possibile esportare le divisioni in titolari separati e importare i dati in un ambiente pubblico. Lo strumento di esportazione registra il processo e visualizza la directory di output del file di registro al termine dell'esportazione. Il processo di esportazione registra l'output corretto di ogni tabella e indica le eventuali condizioni o gli errori imprevisti rilevati.

Importante È possibile effettuare solo la migrazione di divisioni da CA Automazione supporto r6.0 SR1 eFix5.

Per esportare dati CA Automazione supporto

1. Eseguire lo script `SA60Export` dal supporto di installazione nella directory seguente:

`/casd.nt/SAMigration`

Nota: l'estensione file dipende dal sistema operativo. In Windows, ad esempio, viene utilizzato "bat", in UNIX viene utilizzato "sh" per lo script bourne shell, "csh" per la C shell o "ksh" per la Korn shell e così via.

Viene visualizzato lo strumento di migrazione di CA Automazione supporto.

2. Procedere come segue:
 - a. Immettere la directory principale di installazione di CA Automazione supporto r6.0 SR1 eFix5 "WEB-INF".
 - b. Immettere una directory in cui esportare i dati CA Automazione supporto.

Nota: al termine dell'esportazione, spostare questa cartella nella directory `NX_ROOT/site/sbmigration/SA60` sul server CA Service Desk Manager.

- c. (Facoltativo) Specificare se è possibile esportare le password. Se si seleziona questa opzione, le password vengono esportate per gli utenti, le credenziali predefinite e le credenziali delle attività automatizzate.
- d. (Facoltativo) Esportare una o tutte le divisioni. Se si seleziona questa opzione, viene visualizzato un elenco a discesa con tutte le divisioni attive.

3. Fare clic su Esegui.

Nello Stato processo vengono visualizzate informazioni sull'esportazione, ad esempio la tabella di database migrata, e il numero dei record nella tabella.

Se lo strumento rileva errori irreversibili, viene visualizzato un messaggio.

Nota: è possibile interrompere l'esportazione selezionando Interrompi dalla barra degli strumenti o dal menu File.

Verrà completata l'esportazione dei dati.

4. Configurare e implementare Automazione supporto, nel modo appropriato per il proprio ambiente.

Nota: per ulteriori informazioni sulla configurazione delle opzioni di Automazione supporto, vedere la *Guida in linea*.

Importazione di dati Automazione supporto

Per importare dati Automazione supporto è necessario convertirli prima in formato *.DAT*. È possibile importare i dati in CA Service Desk Manager utilizzando lo script di migrazione di Automazione supporto. Richiamare l'utilità dopo aver installato e configurato CA Service Desk Manager. È inoltre possibile eseguire *sa_migrate.pl* utilizzando il comando *pdm_perl*.

È possibile accedere allo script nella directory *NX_ROOT\bin*. Lo script di migrazione esegue attività quali l'elaborazione delle tabelle per mantenere i vincoli del database, crea oggetti CA Service Desk Manager corrispondenti, mappa i valori delle colonne con titolare e così via.

La posizione predefinita per i file relativi alla migrazione nell'installazione di CA Service Desk Manager è la directory *NX_ROOT/site/sbmigration*. Il file di configurazione importato si trova ad esempio nella cartella *NX_ROOT/site/sbmigration/config*. Nel file *sa_migration_config.dat* sono memorizzate le colonne *id*, *prop_name*, *value* e *prop_description* nel formato di dati di CA Service Desk Manager.

Nella directory sono archiviati i dati di esportazione di CA Automazione supporto r6.0 SR1 eFix5, il codice dell'utilità di migrazione, gli script Perl e così via.

Per importare dati Automazione supporto

1. Avviare il servizio CA Service Desk Manager.

Il servizio viene avviato ed è possibile verificare che sia in esecuzione.

2. Immettere quanto segue nella riga di comando:

```
pdm_perl <NX_ROOT>\bin\sa_migrate.pl
```

I dati Automazione supporto vengono caricati nel database dal pacchetto di esportazione.

Modalità di configurazione dell'accesso previsto dal ruolo di Automazione supporto dopo la migrazione

Se si configura Automazione supporto prima della migrazione, l'accesso previsto dal ruolo viene configurato correttamente. Se si configura Automazione supporto dopo la migrazione, impostare il campo di accesso a Automazione supporto per ogni ruolo sul valore appropriato. Se l'accesso previsto dal ruolo non viene impostato correttamente, non sarà possibile accedere all'interfaccia utente finale o analista di Automazione supporto.

Nel processo seguente viene descritto come configurare l'accesso previsto dal ruolo Automazione supporto dopo la migrazione:

1. Installare l'opzione *supportautomation_url*.

2. Impostare il campo relativo all'accesso per ogni ruolo per il quale si desidera concedere l'accesso a Automazione supporto.

Nota: per ulteriori informazioni sull'installazione dell'opzione *supportautomation_url* o sulla creazione di ruoli di accesso a Automazione supporto, vedere la *Guida in linea*.

Modalità di migrazione di un universo CA Business Intelligence personalizzato

È possibile migrare un universo personalizzato nel modo seguente:

1. Seguire le istruzioni per collegare un universo personalizzato all'universo CA Service Desk Manager.
2. Eseguire il backup del file *biar* di qualsiasi universo o report definito a livello di sito.
3. Installare un universo dalla versione corrente.
4. Collegare l'universo personalizzato all'universo dalla versione corrente.

Modalità di esecuzione del backup di un universo personalizzato

Se si è collegato un universo personalizzato all'universo di CA Service Desk Manager, effettuare le seguenti operazioni prima di installare l'universo e i report r12.5:

1. Utilizzare la procedura guidata di importazione per creare un file di backup *biar* di qualsiasi universo o report definito a livello di sito.
2. Avviare Universe Designer.
3. Importare l'universo personalizzato.
4. Salvare una copia dell'universo sull'unità locale.

Viene eseguito il backup dell'universo personalizzato.

Ulteriori informazioni:

[Passaggio da sviluppo a produzione](#) (a pagina 405)

Installazione di un universo CA Business Intelligence

L'installazione dell'universo viene eseguita per sostituire l'universo e i report di CA Business Intelligence r12.0.

Per installare l'universo

1. Dal secondo DVD di CA Service Desk, eseguire il file setup.exe.
2. Selezionare la scheda Installazione prodotto.
3. Scorrere verso il basso e selezionare l'opzione di configurazione di CA Business Intelligence.

Viene visualizzata la procedura guidata di installazione dei componenti di CA Service Desk.

4. Fare clic su Avanti e immettere le credenziali utente.

Nota: se CA Service Desk Manager non è installato sul computer, specificare il nome host CA Service Desk Manager.

5. Fare clic su Fine.

L'universo e i report di CA Business Intelligence r12.0 vengono sostituiti e nelle sottocartelle vengono creati i report r12.5.

Aggiornamento del collegamento a un universo

Anche se il nome dell'universo rimane invariato in CA Service Desk Manager r12.5, è *necessario* aggiornarne il collegamento. In caso contrario, potrebbero verificarsi problemi di connessione all'universo quando si eseguono i report e si importa l'universo. Potrebbe essere visualizzato il messaggio di errore seguente:

Impossibile risolvere L'ID universo principale

Per aggiornare il collegamento all'universo

1. Avviare Universe Designer sullo stesso computer utilizzato per eseguire il backup dell'universo personalizzato.
2. Selezionare File, Open per aprire l'universo personalizzato.
3. Selezionare File, Parameters.

Viene visualizzata la finestra di dialogo Universe Parameters.

4. Fare clic sulla scheda Links.
5. Nella colonna Name, fare clic sull'universo CA Service Desk Manager.
Il pulsante Change Source diventa attivo.
6. Fare clic sul pulsante Change Source.

7. Individuare e selezionare la posizione del file `.unv` di CA Service Desk Manager.

Nota: generalmente il file `.unv` si trova nella cartella CA Universes.

8. Fare clic su Open, quindi su OK.

Il collegamento all'universo viene aggiornato.

9. Esportare l'universo personalizzato.

Configurazione post aggiornamento

È possibile configurare il prodotto al completamento dell'aggiornamento. Utilizzare la configurazione guidata per verificare le personalizzazioni esistenti.

Nota: se la finestra di dialogo Configurazione si chiude senza completare la configurazione post aggiornamento, eseguire `pdm_configure -s` dalla riga di comando.

Modalità di aggiornamento di CA Workflow e CA EEM

In CA Service Desk Manager r12.5 CA Workflow e CA EEM vengono installati separatamente.

Quando si effettua la migrazione a r12.5, è necessario eseguire l'aggiornamento ad almeno CA EEM r8.3 e CA Workflow r1.1.5.

Nota: è possibile aggiornare da CA EEM r8.1 direttamente a r8.4 SP3.

Per aggiornare CA EEM e CA Workflow, effettuare le seguenti operazioni:

1. Verificare che l'aggiornamento a CA Service Desk Manager r12.5 sia stato completato correttamente.
2. Inserire il supporto di installazione nella propria unità.
3. Installare CA EEM.

Nota: è possibile installare CA EEM dal supporto di installazione oppure scaricare il programma di installazione da [CA Support Online](#).

4. Installare CA Workflow.

Dopo avere installato CA Workflow e CA EEM, è *necessario* impostare manualmente le opzioni appropriate in Gestione opzioni. Rivedere le opzioni aggiornate con attenzione, poiché la porta Tomcat predefinita per CA Workflow non è più la porta 8080 e l'URL predefinito di Gestione processi non è più pmService.

Nota: il nuovo valore predefinito dell'opzione *cawf_pm_url* è cambiato in *http://<wf_hostname>:<wf_tomcat_port>/pm/service/pmService2*. È pertanto *necessario* cambiare manualmente "pmService" in "pmService2" per garantire le comunicazioni CAWF.

Importante Dopo avere aggiornato CA EEM, è *necessario* impostare le opzioni *eiam_hostname*, *use_eiam_artifact* e *use_eiam_authentication* in Gestione opzioni, Sicurezza se in precedenza è stato utilizzato eIAM per l'autenticazione degli utenti CA Service Desk Manager. Per ulteriori informazioni sulle opzioni, consultare la *Guida in linea*.

Cancellazione dei dati nella cache del motore Web e del browser

Dopo avere eseguito l'aggiornamento a CA Service Desk Manager r12.5, eseguire l'utilità *pdm_webcache* per cancellare i dati nella cache per il motore web e il browser. Se nella versione precedente erano presenti moduli personalizzati, è necessario eseguire *pdm_webcache* dopo avere eseguito lo script *migrate_to_r12_5_web_check.pl*.

Nota: se nella versione precedente non erano presenti moduli personalizzati, è possibile eseguire l'utilità immediatamente dopo il completamento della configurazione di CA Service Desk Manager.

pdm_webcache -b -H

-b

Avvisa l'utente di cancellare i dati nella propria cache del browser.

-H

Cancella i dati nella cache del motore Web.

Configurazione di directory e server Web

In seguito all'aggiornamento, è consigliabile configurare Web Director, il server primario e tutti i server secondari.

Per configurare Web Director e i server

1. Se la versione precedente è stata configurata per l'utilizzo di server secondari o di web director, eseguire lo script seguente:

```
$NX_ROOT\samples\pdmconf\pdm_edit.pl
```

2. Attenersi ai passaggi definiti in *pdm_edit.pl* per completare la configurazione.

Nota: i server secondari e Web Director non possono funzionare finché non si esegue *pdm_edit.pl* in un sistema aggiornato.

Attività successive alla migrazione LREL

Al termine della migrazione, completare i passaggi di verifica seguenti:

1. Eseguire una query sul contenuto delle nuove tabelle per verificare che contengano i dati corretti.
2. Aggiornare ciascun report definito a livello di sito per verificare che i dati del report provengano dalle nuove tabelle LREL.
3. Verificare i report definiti a livello di sito.

Oggetti e tabelle obsolete

Gli oggetti e le tabelle seguenti sono obsoleti per questa versione di CA Service Desk Manager. Durante la migrazione, i dati vengono copiati nelle tabelle LREL r12.5. Nel sistema vengono utilizzate le tabelle e gli oggetti LREL, ma a scopo di riferimento nelle tabelle precedenti vengono conservati i dati presenti al momento dell'aggiornamento.

Nota: per ulteriori informazioni sulle tabelle LREL, consultare la *Guida di riferimento tecnico*.

Nome DBMS	Nome oggetto
Attachment_Lrel	attmnt_lrel
Business_Management_Repository_ Lrel	bmlrel
Chgcat_Group	chgcat_grp
Chgcat_Loc	chgcat_loc
Chgcat_Workshift	chgcat_workshift
Group_Loc	grp_loc
Isscat_Group	isscat_grp
Isscat_Loc	isscat_loc
Isscat_Workshift	isscat _workshift
Knowledge_Lrel_Table	kmlrel
Lrel_Table	lrel1
Pcat_Group	pcat_grp
Pcat_Loc	pcat_loc
Pcat_Workshift	pcat_workshift
Wftpl_Group	wftpl_grp

Tabelle e oggetti LREL

La migrazione crea automaticamente le tabelle e gli oggetti seguenti per gestire relazioni dati di tipo molti a molti:

Nome DBMS	Nome oggetto
usp_lrel_asset_chgnr	lrel_asset_chgnr
usp_lrel_asset_issnr	lrel_asset_issnr
usp_lrel_att_cntlist_macro_ntf	lrel_att_cntlist_macro_ntf
usp_lrel_att_ctplist_macro_ntf	lrel_att_ctplist_macro_ntf
usp_lrel_att_ntflist_macro_ntf	lrel_att_ntflist_macro_ntf
usp_lrel_attachments_changes	lrel_attachments_changes
usp_lrel_attachments_issues	lrel_attachments_issues
usp_lrel_attachments_requests	lrel_attachments_requests
usp_lrel_aty_events	lrel_aty_events
usp_lrel_bm_reps_assets	lrel_bm_reps_assets
usp_lrel_bm_reps_bmhiers	lrel_bm_reps_bmhiers
usp_lrel_cenv_cntref	lrel_cenv_cntref
usp_lrel_dist_cntlist_mgs_ntf	lrel_dist_cntlist_mgs_ntf
usp_lrel_dist_ctplist_mgs_ntf	lrel_dist_ctplist_mgs_ntf
usp_lrel_dist_ntflist_mgs_ntf	lrel_dist_ntflist_mgs_ntf
usp_lrel_false_action_act_f	lrel_false_action_act_f
usp_lrel_false_bhv_false	lrel_false_bhv_false
usp_lrel_kwrds_crsolref	lrel_kwrds_crsolref
usp_lrel_notify_list_cntchgntf	lrel_notify_list_cntchgntf
usp_lrel_notify_list_cntissntf	lrel_notify_list_cntissntf
usp_lrel_notify_list_cntntf	lrel_notify_list_cntntf
usp_lrel_ntfr_cntlist_att_ntfrlist	lrel_ntfr_cntlist_att_ntfrlist
usp_lrel_ntfr_ctplist_att_ntfrlist	lrel_ntfr_ctplist_att_ntfrlist
usp_lrel_ntfr_macrolist_att_ntfrlist	lrel_ntfr_macrolist_att_ntfrlist
usp_lrel_ntfr_ntflist_att_ntfrlist	lrel_ntfr_ntflist_att_ntfrlist
usp_lrel_oenv_orgref	lrel_oenv_orgref
usp_lrel_status_codes_tsktypes	lrel_status_codes_tsktypes

usp_lrel_svc_grps_svc_chgcat	lrel_svc_grps_svc_chgcat
usp_lrel_svc_grps_svc_isscat	lrel_svc_grps_svc_isscat
usp_lrel_svc_grps_svc_pcat	lrel_svc_grps_svc_pcat
usp_lrel_svc_grps_svc_wftpl	lrel_svc_grps_svc_wftpl
usp_lrel_svc_locs_svc_chgcat	lrel_svc_locs_svc_chgcat
usp_lrel_svc_locs_svc_groups	lrel_svc_locs_svc_groups
usp_lrel_svc_locs_svc_isscat	lrel_svc_locs_svc_isscat
usp_lrel_svc_locs_svc_pcat	lrel_svc_locs_svc_pcat
usp_lrel_svc_schedules_chgcat_svc	lrel_svc_schedules_chgcat_svc
usp_lrel_svc_schedules_isscat_svc	lrel_svc_schedules_isscat_svc
usp_lrel_svc_schedules_pcat_svc	lrel_svc_schedules_pcat_svc
usp_lrel_true_action_act_t	lrel_true_action_act_t
usp_lrel_true_bhv_true	lrel_true_bhv_true

Verifica della conversione LREL

Durante la migrazione dei dati, vengono aggiunte tabelle LREL per gestire le relazioni molti-a-molti. È possibile verificare il contenuto delle nuove tabelle nonché del codice e dei report aggiornati definiti a livello di sito.

Per verificare i dati nelle tabelle LREL

1. Eseguire una query sul contenuto delle tabelle per verificare che contengano i dati corretti.
2. Aggiornare ciascun report definito a livello di sito per verificare che i dati del report provengano dalle nuove tabelle LREL.
3. Aggiornare le query con i nuovi riferimenti di tabella DBMS.
4. Verificare i report e il codice definiti a livello di sito. Aggiornare il codice in modo da utilizzare le nuove tabelle LREL e un'interfaccia supportata, ad esempio Servizi Web. Se necessario, aggiornare i nomi di tabella nel codice.

Verifica delle personalizzazioni del database

È possibile verificare che le personalizzazioni del database siano state migrate correttamente nella versione corrente del prodotto.

Per verificare le personalizzazioni del database

1. Esaminare ogni tabella personalizzata utilizzando il prodotto di gestione del database o Screen Painter Web.
2. Verificare che i file personalizzati vengano visualizzati nella directory seguente:

`$NX_ROOT/site/mods/`

Verifica delle personalizzazioni del modulo Web

È possibile verificare che le personalizzazioni dei moduli Web siano state migrate correttamente nella versione corrente del prodotto.

Per verificare le personalizzazioni dei moduli Web

1. Verificare che i moduli personalizzati vengano visualizzati nella directory `$NX_ROOT/site/mods/www/html/`.
2. Verificare che il modulo Web venga aperto correttamente all'interno di un browser.
3. Verificare che il modulo Web venga aperto correttamente in Web Screen Painter.

Modifica dei tipi accesso

Quando si effettua l'aggiornamento da CA Service Desk Manager r11.2, il processo di aggiornamento crea automaticamente ruoli per tutti i tipi di accesso e assegna correttamente a tali ruoli accesso e autorizzazioni. Per sfruttare i vantaggi dei nuovi ruoli nella versione r12.5, è possibile creare ruoli per i tipi di accesso.

Per creare ruoli per i tipi di accesso

1. Accedere all'interfaccia Web come utente con possibilità di accedere alla scheda Amministrazione.
2. Fare clic sulla scheda Amministrazione.
3. Nella struttura a sinistra selezionare Gestione ruoli e protezione, Tipi di accesso.

Vengono visualizzati tutti i tipi di accesso disponibili.

4. Fare clic su un tipo di accesso disponibile.

Viene visualizzata la pagina dei dettagli per il tipo di accesso selezionato.

5. Fare clic sulla scheda Ruoli.
6. Selezionare un nuovo ruolo per il tipo di accesso e fare clic su Aggiorna ruoli.

Il nuovo ruolo viene associato al tipo di accesso.

Nota: è inoltre possibile creare un ruolo personalizzato e assegnarlo al tipo di accesso. Per informazioni sulla creazione dei ruoli, consultare la *Guida all'amministrazione*.

Abilitare Calcolo priorità

Calcolo priorità è un set di valori che consentono di impostare automaticamente i valori di Priorità, Urgenza e Impatto per i problemi e gli incidenti. Per impostazione predefinita, nelle nuove installazioni di CA Service Desk Manager è abilitato il calcolo priorità predefinito per i tipi di ticket problema e incidente. Se, tuttavia, si esegue l'aggiornamento da una versione precedente, tale calcolo non risulta attivo.

Se si crea e si attiva un calcolo priorità differente, i valori dei ticket rifletteranno le impostazioni del calcolo priorità attivo associato a un incidente o un problema. Se non è attivo alcun calcolo priorità, gli utenti possono impostare manualmente la Priorità e altri valori sui ticket.

Nota: i moduli personalizzati dell'interfaccia Dipendente e Cliente funzionano in modo analogo alle versioni precedenti. Gli utenti self-service possono modificare direttamente la Priorità indipendentemente dalle impostazioni del calcolo priorità.

Per abilitare il calcolo priorità in seguito alla migrazione, effettuare le operazioni seguenti:

1. Nella scheda Amministrazione, passare a Service Desk, Richieste/Incidenti/Problemi, Calcolo priorità.
Viene visualizzato l'elenco Calcolo priorità.
2. Fare clic con il pulsante destro del mouse sul calcolo priorità predefinito o su un altro calcolo priorità e selezionare Modifica dal menu di scelta rapida.
Viene visualizzata la pagina Aggiorna calcolo priorità.
3. Impostare lo stato su Attivo.
4. Selezionare uno o più dei tipi di ticket seguenti:

Incidenti

Consente di gestire i ticket incidente con questo calcolo priorità. Gli incidenti possono essere gestiti da un solo calcolo priorità attivo.

Problemi

Consente di gestire i ticket problema con questo calcolo priorità. I problemi possono essere gestiti da un solo calcolo priorità attivo.

5. Fare clic su Salva.

I valori del calcolo priorità predefinito sono applicabili ai nuovi ticket a meno che non sia stato attivato un altro calcolo priorità. Nei nuovi ticket che utilizzano un calcolo priorità, il campo Priorità è di sola lettura.

Nota: per informazioni sulla definizione di un calcolo priorità per titolari e ticket, consultare la *Guida all'amministrazione* e la *Guida in linea*.

Modalità di aggiunta del campo Priorità incidente agli incidenti

La *priorità incidente* è rappresentata dalla somma dei valori di urgenza e impatto. Tale priorità è valida solo per il tipo di ticket incidente. Il valore Priorità incidente viene visualizzato negli incidenti dopo aver installato l'opzione use_incident_priority e averla aggiunta al modulo della pagina Dettagli incidente con Screen Painter Web.

Per aggiungere un campo Priorità incidente all'incidente, effettuare le operazioni seguenti:

1. Installare l'opzione use_incident_priority da Gestione opzioni, Gestione richiesta.
2. Utilizzare Screen Painter Web per aggiungere il campo Priorità incidente alle pagine Dettagli incidente.

Se l'opzione use_incident_priority è installata, nella pagina Dettagli incidente salvata viene visualizzato il valore Priorità incidente. Quando non è installata l'opzione use_incident_priority, il valore Priorità incidente è zero.

Nota: l'opzione use_incident_priority consente di gestire solo il valore Priorità incidente e non è correlata al calcolo priorità.

Ulteriori informazioni:

[Impostazione dell'intervallo di urgenza per gli utenti self-service](#) (a pagina 56)

Aggiunta del campo Urgenza ai ticket dipendente

Per impostazione predefinita, il campo Urgenza non viene visualizzato negli incidenti o nelle richieste di tipo Dipendente. È tuttavia possibile aggiungere il campo Urgenza utilizzando l'opzione `urgency_on_employee`.

Nota: quando si disinstalla l'opzione `urgency_on_employee` e si disabilita il calcolo priorità, il campo Priorità viene visualizzato nelle pagine Dettagli richiesta e Dettagli incidente per gli utenti self-service.

Per aggiungere il campo Urgenza ai ticket Dipendente, installare l'opzione `urgency_on_employee` da Gestione opzioni, Gestione richieste. Il campo Urgenza viene visualizzato negli incidenti o nelle richieste di tipo Dipendente. Gli utenti self-service possono ignorare il valore dell'incidente.

Modalità di impostazione dei valori del ticket per gli utenti self-service

È possibile controllare i valori di urgenza e di priorità visualizzati agli utenti self-service. Le priorità impostate nel file `web.cfg` consentono di gestire le opzioni che vengono mostrate agli utenti durante la creazione o la modifica dei ticket.

Per impostare i valori dei ticket per gli utenti self-service, tenere presente quanto segue:

1. Per ogni valore di sostituzione nel parametro di `web.cfg`, specificare uno o più valori.
2. Per i [valori di urgenza](#) (a pagina 57), specificare uno o più numeri compresi tra 0 e 4.
3. Per i [valori di priorità](#) (a pagina 58), specificare uno o più numeri compresi tra 1 e 5 o la parola Nessuno.
4. Separare ogni valore con uno spazio.
5. Specificare il primo valore dell'elenco come valore predefinito visualizzato nei ticket. Se necessario, è possibile ripetere il valore predefinito nell'elenco per migliorare la leggibilità.

Ulteriori informazioni:

[Impostazione dell'intervallo di urgenza per gli utenti self-service](#) (a pagina 56)

[Valori della proprietà Urgenza](#) (a pagina 57)

[Impostare l'intervallo di priorità per gli utenti self-service](#) (a pagina 57)

[Valori della proprietà Priorità](#) (a pagina 58)

Impostazione dell'intervallo di urgenza per gli utenti self-service

Per gli incidenti e le richieste self-service, è possibile impostare valori di urgenza predefiniti nel file *web.cfg*. Quando si imposta un intervallo di valori di urgenza, gli utenti self-service quali i dipendenti, i dipendenti VIP o i guest possono impostare valori di urgenza sui ticket. Le opzioni disponibili per gli utenti self-service si basano sull'intervallo di valori impostato nel file *web.cfg*.

Per impostare l'intervallo di urgenza predefinito per gli utenti self-service

1. Aprire il file *web.cfg* nella directory appropriata:
 - (Windows) %NX_ROOT%\bopcfg\www\
 - (UNIX) \$NX_ROOT/bopcfg/www/
2. Per ogni parametro, specificare uno o più [valori per la proprietà di urgenza](#) (a pagina 57). Separare ogni valore con uno spazio.

ESCEmpUrg

Specifica in che modo i dipendenti VIP possono ignorare l'urgenza dei ticket.

EmpUrg

Specifica in che modo i dipendenti possono ignorare l'urgenza dei ticket.

AnonymousUrg

Specifica priorità valide per ticket creati da utenti guest.

3. Salvare il file *web.cfg*.
Nei nuovi ticket i dipendenti, i dipendenti VIP o i guest possono impostare valori di urgenza basati sull'intervallo di valori del file *web.cfg*.

Esempio: Mostra ai guest solo due valori di urgenza in una richiesta

1. Aprire il file *web.cfg*.
2. Impostare il parametro *AnonymousUrg* su 0 4, ad esempio *AnonymousUrg* 0 4.
3. Salvare il file *web.cfg*.

I valori di urgenza visualizzati all'utente self-service sono 1-Appena possibile e 5-Immediato. Il valore di urgenza predefinito è 1-Appena possibile.

Valori della proprietà Urgenza

Nel file *web.cfg* sono contenute impostazioni che consentono di controllare in che modo gli utenti self-service possono ignorare l'urgenza sui ticket. Sono disponibili i valori seguenti per la proprietà di urgenza:

- **0**: consente all'utente di impostare l'Urgenza su 1-Appena possibile
- **1**: consente all'utente di impostare l'Urgenza su 2-Presto
- **2**: consente all'utente di impostare l'Urgenza su 3-Rapidamente
- **3**: consente all'utente di impostare l'Urgenza su 4-Molto rapidamente
- **4**: consente all'utente di impostare l'Urgenza su 5-Immediato

Impostare l'intervallo di priorità per gli utenti self-service

È possibile impostare un intervallo di priorità valide per consentire agli utenti self-service di ignorare i valori di priorità sui ticket. Quando si imposta l'intervallo di priorità, i clienti, i dipendenti o i guest possono impostare valori di priorità basati sull'intervallo di valori del file *web.cfg*.

Per impostare l'intervallo di priorità per gli utenti self-service

1. Nel file *web.cfg* contenuto nella directory appropriata:
 - (Windows) %NX_ROOT%\bopcfg\www\
 - (UNIX) \$NX_ROOT/bopcfg/www/
2. Per ognuno dei parametri, specificare uno o più [valori della proprietà Priorità](#) (a pagina 58).

CstPrio

Specifica in che modo i dipendenti possono ignorare la priorità sui ticket.

EmpPrio

Specifica in che modo i dipendenti possono ignorare la priorità sui ticket.

AnonymousPrio

Specifica in che modo i dipendenti possono ignorare la priorità sui ticket.

3. Salvare il file *web.cfg*.

Nei nuovi ticket i clienti, i dipendenti o i guest possono impostare valori di priorità basati sull'intervallo di valori del file *web.cfg*.

Esempio: Mostra ai guest solo sue valori di priorità

1. Aprire il file *web.cfg*.
2. Impostare il parametro *AnonymousPrio* su None 4. Ad esempio:
AnonymousPrio None 4.
3. Salvare il file *web.cfg*.

Quando un guest utilizza i ticket, i valori per l'urgenza sono Nessuno o 4. Il valore predefinito è Nessuno.

Valori della proprietà Priorità

Nel file *web.cfg* sono contenute impostazioni che consentono di controllare in che modo gli utenti self-service possono ignorare il ticket Priorità. Sono disponibili i valori seguenti per la proprietà Priorità:

- **Nessuno:** consente all'utente di impostare la Priorità su Nessuno
- **1:** consente all'utente di impostare la Priorità su 1 (priorità massima)
- **2:** consente all'utente di impostare la Priorità su 2
- **3:** consente all'utente di impostare la Priorità su 3
- **4:** consente all'utente di impostare la Priorità su 4
- **5:** consente all'utente di impostare la Priorità su 5 (priorità massima)

Attivazione di transizioni di stato

Al termine dell'aggiornamento, tutte le transizioni di stato predefinite non sono attive. È possibile attivarle e modificarle in modo da ottenere il flusso di transizioni di stato dei ticket desiderato.

Nota: tutte le descrizioni di codice di stato personalizzate che compaiono in moduli di ticket vengono trattenute durante il processo di aggiornamento.

Per attivare una transizione di stato

1. Nella scheda Amministrazione, espandere il nodo Service Desk e selezionare uno dei tipi di ticket seguenti:
 - Ordini di cambiamento
 - Transizioni Ordine di cambiamento

- Questioni
 - Transizioni Questione
- Richieste/Incidenti/Problemi:
 - Transizioni Incidente
 - Transizioni Problema
 - Transizioni richiesta

Viene visualizzato l'elenco relativo alle transizioni.

2. Selezionare Mostra filtro nella pagina dell'elenco transizioni.

Nella parte superiore della pagina sono visualizzati i campi di ricerca aggiuntivi.

3. Nel campo Stato record, selezionare Non attivo e fare clic su Cerca.

Nell'elenco delle transizioni in fondo alla pagina vengono visualizzate le transizioni inattive.

4. Aprire la transizione per la modifica.
5. Nell'elenco a discesa Stato record, selezionare Attivo.
6. Fare clic su Salva e chiudere la finestra.
7. Fare clic su Ricerca.

Nell'elenco delle transizioni viene visualizzata la transizione attiva.

Nota: per ulteriori informazioni sulle transizioni di stato, consultare la *Guida all'amministrazione* e la *Guida in linea*.

Attivazione di tipi di transizione

Per impostazione predefinita, tutti i tipi di transizione predefiniti forniti con il prodotto non sono attivi, pertanto i pulsanti di transizione di stato non sono abilitati. È possibile attivare e modificare questi tipi di transizione in modo da ottenere il flusso di transizioni di stato desiderato.

Per attivare una transizione di stato

1. Selezionare Mostra filtro nella pagina Elenco Tipi di transizione.

Nella parte superiore della pagina sono visualizzati i campi di ricerca aggiuntivi.

2. Nel campo Stato record, selezionare Non attivo e fare clic su Cerca.

L'Elenco Tipi di transizione visualizza tutti i tipi di transizione non attivi.

3. Fare clic con il pulsante destro del mouse sul nome del tipo di transizione e, nel menu visualizzato, selezionare Modifica.

4. Nell'elenco a discesa Stato record, selezionare Attivo.
5. Fare clic su Salva e chiudere la finestra.
6. Fare clic su Ricerca.

L'Elenco Tipi di transizione mostra il tipo di transizione attivo.

Personalizzazione di aree di accesso funzionali

Un'area di accesso funzionale è un gruppo di oggetti che consentono di limitare l'accesso utente. Nelle versioni precedenti di CA Service Desk Manager sono disponibili otto gruppi di accesso funzionale fissi per limitare l'accesso ai componenti di codice.

Durante la migrazione, i gruppi di accesso funzionale migrano nelle nuove aree di accesso funzionali per ogni ruolo. La migrazione gestisce automaticamente le modifiche Majic, i dati di riferimento predefiniti e il mapping dei ruoli alle nuove aree di accesso funzionali.

Al termine della migrazione, procedere nel modo seguente:

- Esaminare il mapping degli oggetti alle aree di accesso funzionali esistenti e nuove e alle autorizzazioni di ruolo di ogni area. Utilizzare Screen Painter Web per verificare le aree di accesso funzionali.
- Utilizzare CA Service Desk Manager per rimappare o modificare le autorizzazioni. Verificare che gli utenti dispongano dell'accesso appropriato alle funzionalità e agli oggetti.

Nota: per informazioni dettagliate sulle autorizzazioni predefinite e sulla mappatura degli oggetti alle nuove aree di accesso funzionali, vedere il sito Web del supporto per i prodotti. Per informazioni sulla modifica o l'aggiunta delle aree di accesso funzionali, vedere la *Guida in linea*.

Nella tabella seguente le aree di accesso funzionali vengono mappate ai componenti di codice:

Area di accesso funzionale	Componente di codice	Nuovo
Amministrazione	amministrazione	No
Incidente/Problema/Richiesta	call_mgr	No
Ordine di cambiamento	change_mgr	No
Inventario	inventario	No
Questione	issue_mgr	No
Documento della conoscenza	kd	No

Notifica	notifica	No
Riferimento	riferimento	No
Protezione	protezione	No
Annuncio	annuncio	Sì
Riferimento Incidente/Problema/Richiesta	call_mgr_reference	Sì
Modello Incidente/Problema/Richiesta	call_mgr_template	Sì
Modello Ordine di cambiamento	change_mgr_template	Sì
Riferimento Ordine di cambiamento	change_reference	Sì
Elemento di configurazione	ci	Sì
Elemento di configurazione comune	ci_common_ro	Sì
Riferimento elemento di configurazione	ci_reference	Sì
Contatto	contatto	Sì
Gruppo	gruppo	Sì
modello questione	issue_mgr_template	Sì
Riferimento Questione	issue_reference	Sì
Ubicazione	ubicazione	Sì
Amministrazione sito multiplo	multisite_admin	Sì
Riferimento sito multiplo	multisite_reference	Sì
Riferimento notifica	notification_reference	Sì
Organization	organizzazione	Sì
Prioritizzazione	prioritizzazione	Sì
Livello di servizio	service_level	Sì
Sito	sito	Sì
Query memorizzata	stored_queries	Sì
Indagine	indagine	Sì
Amministratore titolare	tenant_admin	Sì
Fuso orario	timezone	Sì
Riferimento flusso di lavoro	workflow_reference	Sì
Turno	turni	Sì

Modifiche a livello di accesso post migrazione

Al termine della migrazione, è possibile verificare i livelli di accesso funzionale per ogni ruolo. Poiché gli oggetti sono stati spostati in altre aree di accesso funzionali, in determinate situazioni è possibile che l'utente sia in grado di accedere ad alcune schermate il cui accesso non era in precedenza consentito. Analogamente, potrebbe non disporre di accesso ad alcuni moduli ai quali poteva accedere in passato. Entrambe le situazioni possono verificarsi quando una nuova area di accesso funzionale gestisce le autorizzazioni per due delle aree di accesso funzionali originali.

Nota: per informazioni dettagliate sulle autorizzazioni predefinite e sulla mappatura degli oggetti alle nuove aree di accesso funzionali, vedere il sito Web del supporto per i prodotti. Per informazioni sulla modifica o l'aggiunta dei livelli di accesso, vedere la *Guida in linea*.

File SITEMODS.JS

Per consentire il funzionamento del codice, è necessario che qualsiasi riga di codice aggiunta al file `sitemods.js` della versione precedente e richiamata da una pagina HTML venga inserita nel file `sitemods.js` della versione corrente.

Regolazione dei tipi di accesso

Se nella versione precedente di CA Service Desk Manager sono stati personalizzati tipi di accesso e partizioni dati, dopo l'aggiornamento potrebbero verificarsi alcuni problemi con le impostazioni delle partizioni dati di Gestione delle informazioni. Nelle categorie e nei documenti potrebbero verificarsi problemi con le impostazioni dei gruppi di autorizzazioni. Può, ad esempio, accadere che un utente abbia accesso ad un numero limitato di informazioni.

Nota: anche se, dopo essere stati eliminati, una partizione dati o un tipo di accesso sono stati ricreati, verificarne le impostazioni dopo l'aggiornamento.

Per regolare i tipi di accesso

1. Fare clic sulla scheda Amministrazione.
Viene visualizzata la pagina Amministrazione.
2. Fare clic su Gestione ruoli e protezione, Gestione ruoli, Elenco ruoli.
Viene visualizzato l'Elenco ruoli.

3. Completare la procedura seguente per ciascun ruolo:
 - a. Fare clic con il pulsante destro del mouse sul collegamento e scegliere Modifica.
 - b. Rivedere il campo Nome partizione dati nella scheda Autorizzazione.

Se il campo è vuoto, al tipo di accesso selezionato non sono associate partizioni dati, pertanto l'utente non è soggetto a restrizioni e può accedere a qualsiasi documento o categoria del prodotto, anche se sono stati impostati gruppi di autorizzazioni.

Questa azione può essere appropriata per gli amministratori ma non per tutti i ruoli. Se al ruolo non sono associate partizioni dati, è possibile crearne o modificarne uno.

Regolazione di impostazioni di partizione dati

È possibile modificare i vincoli sulle partizioni dopo aver configurato i ruoli nel sistema. Tale modifica consente di verificare che le autorizzazioni appropriate funzionino correttamente dopo aver eseguito l'aggiornamento alla versione corrente del prodotto.

Per modificare i vincoli sulle partizioni dati

1. Nella scheda Amministrazione visualizzare Gestione protezione e ruoli, Partizione dati, Vincoli partizione dati.

Viene visualizzata la pagina Elenco vincoli partizione dati.
2. Verificare le impostazioni dei vincoli sul codice Majic per le tabelle seguenti:

SKELETONS

Specifica la tabella utilizzata per i documenti di conoscenza.

O_INDEXES

Specifica la tabella utilizzata per le categorie di conoscenza.

Vengono verificate le impostazioni dei vincoli di tabella.

3. Fare clic su Mostra filtro e immettere le Partizioni dati utilizzate in precedenza.

Nota: il campo Nome tabella nell'area di ricerca consente di limitare l'elenco. Ad esempio, inserire *SKELETONS* o *O_INDEXES* nel campo Nome tabella e fare clic sul pulsante Ricerca.

Modifica dei set di file della Guida dopo la migrazione dei ruoli

Dopo l'aggiornamento, in CA Service Desk Manager sono disponibili tutti i ruoli migrati con la *Guida in linea* completa. È possibile modificare i set di file della Guida per qualsiasi ruolo, a seconda delle esigenze del sistema della Guida in linea.

Per modificare i set di file della Guida per un ruolo

1. Nella scheda Amministrazione accedere a Gestione protezione e ruoli, Elenco ruoli.

Viene visualizzata la pagina Elenco ruoli.

2. Aprire il ruolo per la modifica, ad esempio *cliente*.

Viene visualizzata la pagina Dettagli ruolo.

3. Fare clic su Modifica.

4. Selezionare la scheda Interfaccia Web:

Fare clic su Visualizzazione guida.

Viene visualizzato l'elenco dei set di file della Guida disponibili per il ruolo selezionato.

5. Selezionare un set di file della Guida, ad esempio cliente.

6. Salvare il ruolo.

La visualizzazione della guida per il ruolo cambia nel set di file della Guida in linea selezionato.

È possibile visualizzare gli argomenti disponibili in un set di file della Guida in linea anche selezionando i dettagli del set e facendo clic sul pulsante Visualizza guida in linea.

Impostazioni predefinite dei vincoli

Le impostazioni tipiche predefinite per i vincoli sono elencate come segue:

Impostazioni dei vincoli per Partizioni dati cliente e dipendente

Le impostazioni dei vincoli per Partizioni dati cliente e dipendente devono essere:

Tabella SKELETONS

Visualizzare vincoli come:

'SKELETONS READ_PGROU in @root.pgrou or
READ_PGROU.[pgrou] contained_roles.role in @root.id) and
ACTIVE_STATE = 0'

Vincolo di aggiornamento ed eliminazione

'id = 0' (id=0 indica nessun accesso)

Tabella O_INDEXES

Visualizzare vincoli come:

READ_PGROU in @root.pgrou or READ_PGROU.[pgrou]
contained_roles.role in @root.id

Vincolo di aggiornamento ed eliminazione:

WRITE_PGROU in @root.pgrou OR WRITE_PGROU.[pgrou]
contained_roles.role IN @root.role

Impostazioni dei vincoli per analista CA Service Desk Manager, gestori della conoscenza e tecnici della conoscenza

Di seguito vengono riportate le impostazioni dei vincoli per analista CA Service Desk Manager, gestori della conoscenza e tecnici della conoscenza:

Tabella SKELETONS

Visualizzare vincoli come:

(ACTIVE_STATE >= 0)and (READ_PGROU in @root.pgrou or
READ_PGROU.[pgrou] contained_roles.role in @root.id) OR
(ACTIVE_STATE > 0 AND ASSIGNEE_ID = @root.id) OR
(ACTIVE_STATE = 0 AND OWNER_ID = @root.id)) Active

Vincolo di aggiornamento ed eliminazione:

(ACTIVE_STATE >= 0) AND (WRITE_PGROU in @root.pgrou OR
WRITE_PGROU.[pgrou] contained_roles.role IN @root.role) OR
(ACTIVE_STATE > 0 AND ASSIGNEE_ID = @root.id) OR
(ACTIVE_STATE = 0 AND OWNER_ID= @root.id)) Active

Tabella O_INDEXES

Visualizzare vincoli come:

READ_PGROU in @root.pgroups or READ_PGROU.[pgroup]
contained_roles.role in @root.id

Vincolo di aggiornamento ed eliminazione:

WRITE_PGROU in @root.pgroups OR WRITE_PGROU.[pgroup]
contained_roles.role IN @root.role

Avviare l'interfaccia Web IIS (CAisd)

Dopo avere aggiornato un'installazione di CA Service Desk Manager r11.2 Windows con un'integrazione IIS, l'interfaccia Web IIS (CAisd) di CA Service Desk Manager verrà interrotta. Se si desidera continuare ad utilizzare l'integrazione IIS, avviare manualmente CAisd dopo l'aggiornamento.

Importante Se si desidera utilizzare IIS 7.0, è *necessario* installare i componenti di compatibilità metabase e CGI.

Modalità di aggiornamento di Gestione delle informazioni da r11.2

L'aggiornamento a CA Service Desk Manager r12.5 da r11.2 comporta l'aggiornamento automatico dell'ambiente Gestione delle informazioni. Una volta terminato l'aggiornamento, completare i passaggi seguenti:

1. Mappare con il database i collegamenti creati in una risoluzione di documento per individuare collegamenti interrotti.

Nota: per individuare i collegamenti interrotti si utilizzano i criteri *Contrassegna collegamenti interrotti* predefiniti.

2. Fare clic sulla scheda Amministrazione, accedere a Conoscenza, Norme automatiche, Criteri, Pianificazione.

Viene visualizzata la pagina Pianificazione.

3. Selezionare la casella di controllo Esegui calcolo nel campo Ultimo aggiornamento.
4. Immettere una data nella casella di testo Pianificazione oppure fare clic sull'icona Calendario per selezionare una data.
5. Selezionare l'intervallo di tempo per eseguire il calcolo e i criteri. Fare clic su Salva.

I criteri vengono elaborati alla data e all'ora specificate.

6. Eseguire `pdm_k_reindex` come indicato di seguito:

`pdm_k_reindex -pm`

Corregge i collegamenti del documento e le immagini incorporate all'interno del campo della risoluzione.

Importante Dopo l'aggiornamento, è possibile che si verifichi un errore critico quando si esegue `pdm_k_reindex -pm`. In questo caso, accedere a Conoscenza, Gestione processo di approvazione, Impostazioni processo di approvazione e cambiare l'opzione *Autorizzazioni per la modifica del documento dopo la pubblicazione* nel valore che indica che *gli attributi del documento pubblicato possono essere modificati da utenti con autorizzazioni complete*, quindi eseguire `pdm_k_reindex -pm`.

`pdm_k_reindex -ml`

Corregge i collegamenti del documento all'interno del campo della risoluzione e li mappa al database.

`pdm_k_reindex`

Indicizza i documenti consentendo la ricerca all'interno di essi nell'ambiente della conoscenza.

L'ambiente Gestione delle informazioni viene aggiornato a r12.5.

Nota: dopo l'aggiornamento, la stampa dei Documenti della conoscenza può comportare l'inserimento di un grande spazio dopo la sezione Risoluzione del documento. Questo spazio viene inserito a causa di un problema con l'aggiornamento dei modelli di documento da un rilascio precedente. Per maggiori informazioni sulla risoluzione di questo problema di stampa, vedere le *Note di rilascio*.

Importante Una volta effettuato l'aggiornamento, i dati di notifica Gestione delle informazioni da rilasci precedenti di CA Service Desk Manager utilizzano il motore di notifica r12.5. Ad esempio, esistono notifiche di attività predefinite e regole di notifica per tipi di oggetto, come nel caso della scheda Report della conoscenza. Per ulteriori informazioni sull'uso del motore di notifica CA Service Desk Manager da parte di Automazione supporto e Gestione delle informazioni, vedere le *Note di rilascio*.

Ulteriori informazioni:

[Installazione di FAST ESP](#) (a pagina 153)

Modalità di aggiornamento di Gestione delle informazioni da r12 o r12.1

L'aggiornamento di CA Service Desk Manager r12.5 da r12 o r12.1 comporta l'aggiornamento automatico dell'ambiente Gestione delle informazioni. Una volta terminato l'aggiornamento, completare i passaggi seguenti:

1. Mappare al database i collegamenti creati durante la risoluzione di un documento per l'individuazione di collegamenti interrotti.
Nota: per individuare i collegamenti interrotti utilizzare il criterio predefinito *Contrassegna collegamenti interrotti*.
2. Fare clic sulla scheda Amministrazione, accedere a Conoscenza, Norme automatiche, Criteri, Pianificazione.
Viene visualizzata la pagina Pianificazione.
3. Selezionare la casella di controllo Esegui calcolo nel campo Ultimo aggiornamento.
4. Immettere una data nella casella di testo Pianificazione oppure fare clic sull'icona Calendario per selezionare una data.
5. Selezionare l'intervallo di tempo per l'esecuzione del calcolo ed eseguire i criteri.
6. Fare clic su Salva.

I criteri vengono elaborati alla data e all'ora specificate.

7. Per le implementazioni delle ricerche di parole chiave, immettere il comando seguente al prompt dei comandi:

```
pdm_k_reindex
```

8. Per le implementazioni FAST ESP, procedere nel modo seguente:

- a. Caricare il profilo dell'indice r12.5 (file datasearch-5,0-lemmatization.xml) utilizzando la scheda Matching Engines (Motori corrispondenti) dell'interfaccia di amministrazione di FAST ESP.
- b. Riavviare FAST ESP.
- c. Eseguire il comando seguente al prompt dei comandi:

```
pdm_k_reindex factory:all
```

L'ambiente Gestione delle informazioni viene aggiornato a r12.5.

Nota: dopo l'aggiornamento, la stampa dei Documenti della conoscenza può comportare l'inserimento di un grande spazio dopo la sezione Risoluzione del documento. Questo spazio viene inserito a causa di un problema con l'aggiornamento dei modelli di documento da un rilascio precedente. Per maggiori informazioni sulla risoluzione di questo problema di stampa, vedere le *Note di rilascio*.

Importante Una volta effettuato l'aggiornamento, i dati di notifica Gestione delle informazioni da rilasci precedenti di CA Service Desk Manager utilizzano il motore di notifica r12.5. Ad esempio, esistono notifiche di attività predefinite e regole di notifica per tipi di oggetto, come nel caso della scheda Report della conoscenza. Per ulteriori informazioni sull'uso del motore di notifica CA Service Desk Manager da parte di Automazione supporto e Gestione delle informazioni, vedere le *Note di rilascio*.

Ulteriori informazioni:

[Installazione di FAST ESP](#) (a pagina 153)

Capitolo 3: Pianificazione

Questa sezione contiene i seguenti argomenti:

[Elenco delle porte predefinite e consigliate di CA Service Desk Manager](#) (a pagina 71)

[Pianificazione dell'installazione <MDB>](#) (a pagina 74)

[Pianificazione dell'installazione <USD>](#) (a pagina 78)

[Pianificazione dell'installazione di CA EEM e CA Workflow](#) (a pagina 92)

[Pianificazione dell'integrazione di CA IT PAM](#) (a pagina 101)

[Pianificazione dell'installazione di CA Business Intelligence](#) (a pagina 105)

[Pianificazione dell'installazione di CA NSM](#) (a pagina 110)

[Pianificazione dell'installazione di FAST ESP](#) (a pagina 111)

[Strategie di implementazione](#) (a pagina 112)

[Abilitazione dell'autenticazione Windows in Firefox](#) (a pagina 113)

Elenco delle porte predefinite e consigliate di CA Service Desk Manager

L'installazione di CA Service Desk Manager richiede l'apertura di varie porte e intervalli di porte nel firewall. Le informazioni relative alle porte consentono agli amministratori di sito e della protezione di installare e configurare CA Service Desk Manager, nonché le integrazioni con altre soluzioni CA e prodotti di terze parti.

Le porte che è necessario aprire nel firewall dipendono dalle impostazioni del file *NX.env*. Per impostazione predefinita, CA Service Desk Manager sceglie la porta appropriata in base alla disponibilità. Il sistema riserva un numero di porte inferiore a 1024 ma può richiedere fino a 65335 porte.

Le variabili *NX.env* seguenti impostano la porta iniziale (2100) e il tipo di incremento (più 1) utilizzato dal sistema per trovare una porta aperta per l'avvio del processo:

- `NX_SLUMP_FIXED_SOCKETS=1`
- `NX_SLUMP_SECONDARY_SOCKET=2100`

Nell'elenco seguente sono visualizzate le porte (e gli intervalli di porte) predefinite e consigliate per un'installazione tipica di CA Service Desk Manager:

Database

- Oracle: 1521
- SQL Server: 1433

CA Service Desk Manager

- FTP: 21
- SMTP: 25
- HTTP: 80
- HTTPS: 8080
- HTTPS (secondaria): 8081
- POP3: 110
- IMAP: 143
- LDAP: 389
- WebEx: 1270
- mstsc: 1389
- oaserver: 1706
- **Nota:** la porta 1706 è in conflitto con FAST ESP. Per ulteriori informazioni sul conflitto della porta 1706, vedere le *Note di rilascio*.
- Socket slump: 2100
- qserver: 2234
- Socket proctor: 2300
- Comunicazioni: 2365
- Apache Tomcat: 8080
- Arresto di Apache Tomcat:
- SSL su Apache Tomcat: 8443

CA CMDB

- Visualizer: 9080
- Arresto di Apache Tomcat Visualizer: 9085
- CA Cohesion ACM: 9000
- Arresto di CA Cohesion ACM Tomcat: 9005

CA EEM

Porta amministrazione: 5250

CA Workflow

- Apache Tomcat: 8090
- Arresto di Apache Tomcat: 8095

CA Business Intelligence

Nota: per informazioni sulla gestione di porte del firewall per BusinessObjects, vedere BusinessObjects Enterprise XI r2 Deployment and Configuration Guide.

- Apache Tomcat: 8080
- **Consigliata:** 8070
- Reindirizzamento di Apache Tomcat: 8443
- Arresto di Apache Tomcat: 8075
- Arresto di Apache Tomcat secondario: 8005
- Driver ODBC: 1706
- CMS (Central Management Server) BusinessObjects: 8080
- Server applicazioni BusinessObjects: 6400
- ODBC DSN (Database OpenAccess): 1706
- BEA WebLogic: 7001

FAST ESP

- Porta base: 13000
- Interfaccia amministrazione: 16000 (Porta base più 3000)
- Intervallo porte server di licenza: 27000-27009

Nota: è consigliabile non utilizzare l'intervallo di porte 23000-27000, in quanto la porta 27000 viene utilizzata dal server di licenza. Non è possibile cambiare l'intervallo di porte del server di licenza.

Importante FAST ESP utilizza le porte 4000 a partire dalla porta base. Tutte le porte 4000 devono avere accesso illimitato.

Server del portale

- Apache Tomcat: 8080
- Arresto di Apache Tomcat: 8085
- Funzionalità SSL: 8443
- Portal_Safe_List: 8444

Automazione supporto

- Server principale (server socket) interno: 7005
- Server principale (server socket) esterno: 10443
- Server proxy socket (server principale configurazione socket) interno: 7005
- Server proxy socket (server principale configurazione socket) esterno: 10444
- Server routing messaggi (configurazione socket) esterno: 10444
- Apache Tomcat: 8070
- Arresto Apache Tomcat: 8075

Pianificazione dell'installazione <MDB>

Seguire le indicazioni riportate di seguito per la ricerca e la raccolta di informazioni utili per pianificare l'installazione e la configurazione dell'CA MDB in modo corretto.

- **Ricerca** - Leggere *Panoramica di Gestione database di CA* per acquisire familiarità con il database CA MDB, determinare la strategia di distribuzione e ottenere informazioni su eventuali problemi relativi a SQL Server o Oracle, di cui è necessario essere consapevoli per utilizzare con successo il database CA MDB con CA Service Desk Manager.
- **SQL Server**-Per garantire che sia possibile configurare il prodotto e i componenti in SQL Server, completare i seguenti passaggi:
 - Abilitare TCP/IP nel computer in cui si desidera eseguire l'installazione e la configurazione.
 - È necessario disporre delle informazioni seguenti:
 - L'istanza con nome del server su cui è in esecuzione SQL Server.
 - Il nome utente e la password per il database SQL Server.
 - Il numero di porta del database SQL Server.
- **Oracle** - È necessario disporre delle informazioni seguenti:
 - Se il database Oracle è locale o remoto.
 - Se è necessario creare uno spazio tabelle.
 - Il nome del servizio di rete.
 - Il nome utente e la password DBA.
 - Il nome dello spazio tabelle per dati e indice.

- Il percorso completo per lo spazio tabelle.
- Le informazioni di connessione JDBC, inclusi identificatore di sistema (SID) e porta di attesa.

Nota: se non si è sicuri di quali informazioni immettere per il database, vedere la *Guida in linea della configurazione del server*.

Ulteriori informazioni:

[Installazione dell'CA MDB](#) (a pagina 116)

Considerazioni su CA MDB

Prima di installare l'CA MDB, tenere presenti le informazioni seguenti per assicurarsi che l'implementazione venga eseguita correttamente:

- **AIX** - In alcuni computer AIX lo spazio massimo consentito per l'elenco ARG/ENV è troppo ridotto per installare l'CA MDB. Eseguire il comando seguente: `lsattr -l sys0 -ancargs -Fvalue` per trovare l'impostazione attuale per la dimensione massima dell'elenco ARG/ENV. Se il valore restituito è inferiore a 50, è possibile aumentare la dimensione con il comando seguente: `chdev -l sys0 -a ncargs=50`
 - **Oracle** - Tenere presenti le informazioni seguenti:
 - Eseguire una copia di backup di Oracle prima di applicare una patch CA MDB. Il backup può essere eseguito da un database DBA o dallo script della patch. Lo script della patch utilizza la Gestione dei ripristini Oracle (RMAN) per eseguire il backup del database servendosi dell'autenticazione del sistema operativo. La configurazione RMAN potrebbe richiedere che venga abilitata nel database la registrazione dell'archivio (modalità ARCHIVELOG). In alternativa, se per il database DBA è stato eseguito un backup, è possibile eliminare il backup mediante lo script della patch, specificando "no" per il parametro -ORA_BACKUP.
- Nota:** per l'applicazione delle patch viene utilizzato il comando RMAN con l'autenticazione del sistema operativo.
- All'utente Oracle che esegue l'installazione del database CA MDB devono essere assegnati i seguenti privilegi di amministratore di database:
 - Ruolo dba (connettere sys come sysdba; concedere dba all'utente installation_user;).
 - Ruolo sysdba (connettere sys come sysdba; concedere sysdba all'utente installation_user;).

- Concessione di privilegi all'utente mdbadmin per varie tabelle e visualizzazioni di sistema (connettere sys come sysdba; concedere tutti i privilegi su "sys". TABLE_NAME" all'utente installation_user con l'opzione di concessione;). I valori che TABLE_NAME utilizza sono: COL\$, DBA_CONSTRAINTS, DBA_CONS_COLUMNS, DBA_INDEXES, DBA_IND_COLUMNS, DBA_OBJECTS, DBA_OBJECT_TABLES, DBA_REGISTRY, DBA_TABLES, DBA_TABLESPACES, DBA_TAB_COLUMNS, DBA_TAB_PRIVS, DBA_VIEWS, DBMS_REGISTRY, EXPDEPACT\$, EXPDEPOBJ\$, EXPPKGACT\$, EXPPKGOBJ\$, KOPM\$, OBJ\$, TS\$, USER\$
- **Client remoti (UNIX e Linux)** - Quando il database CA MDB viene creato da un client remoto, il processo di creazione del database CA MDB terminerà con un codice restituito di 95 e con il messaggio di errore *"Impossibile creare lo spazio tabelle"* nel registro di installazione, a meno che la directory specificata nel percorso dello spazio tabelle esista sia sul computer client sia sul server Oracle.
- **Componente di installazione dell'CA MDB (SQL)** - Nell'interfaccia del programma di installazione dei componenti dell'CA MDB è visualizzato il campo Nome server database. Tale campo identifica il nome del server locale o il nome del nodo cluster, se in cluster. Utilizzare il nome di rete utilizzato per la connessione a SQL Server.
- **Caratteri speciali (UNIX, Linux e Windows)** - Tenere presenti le informazioni seguenti:
 - (UNIX e Linux) Il nome dell'ID utente dell'amministratore del database utilizzato per creare il database CA MDB non può includere caratteri speciali. Vengono inoltre applicate le restrizioni seguenti:
 - Per i nomi dell'utente e dello spazio tabelle del database DBA sono supportati i caratteri speciali # e _. Qualsiasi altro carattere speciale non è supportato.
 - Per la password DBA e la password MDBADMIN sono supportati i caratteri speciali ~, #, %, ^, -, +, _, {, }, [,], :, . e ? . Qualsiasi altro carattere speciale non è supportato.
 - Per il percorso spazio tabella di Oracle, la directory di destinazione del database MDB, la directory fonte e la directory delle patch del database MDB, sono supportati i caratteri speciali ~, %, ^, _, -, +, [,], {, }, :, (compreso <space> se il percorso è riportato tra virgolette; tuttavia, non sono supportati gli spazi consecutivi).

- (Windows) Il nome dell'ID utente dell'amministratore del database utilizzato per creare il database CA MDB *non può* includere caratteri speciali. Vengono inoltre applicate le restrizioni seguenti:
 - Per i nomi dell'utente e dello spazio tabelle del database DBA sono supportati i caratteri speciali #, \$ e _. Qualsiasi altro carattere non è supportato.
 - Per la password DBA e la password MDBADMIN sono supportati i caratteri speciali ~, !, #, \$, *, (), _, +, `, -, {}, [], \, :, ', ?, ., / e @. Qualsiasi altro carattere non è supportato.
 - Per il percorso spazio tabella di Oracle, la directory di destinazione del database MDB, la directory fonte e la directory delle patch del database MDB, sono supportati i caratteri speciali ~, !, #, \$, (), _, +, `, -, {}, e [] (compreso <space> se il percorso è riportato tra virgolette doppie).
- **Spazi tabelle** - Tenere presenti le informazioni seguenti:
 - Il database CA MDB utilizza lo spazio tabelle temporaneo di sistema per memorizzare le tabelle temporanee. A tal fine, sono necessari almeno 50 megabyte di spazio. Se si sceglie di utilizzare lo spazio tabelle esistente per il database CA MDB, è necessario un minimo di 200 megabyte di spazio disponibile su disco. Nel caso in cui tale spazio non sia disponibile, non è possibile creare il database CA MDB.
 - Se il processo di creazione del database CA MDB viene utilizzato per creare uno spazio tabelle di dati o di indice e il parametro dimensione non è numerico, si verificherà un codice restituito di 350 e nel registro di installazione del database CA MDB sarà segnalato un errore (rc=189) relativo all'impossibilità di creare lo spazio tabelle durante il processo di creazione.
- **Privilegi utente e amministratore** - Il processo di creazione dell'CA MDB non riesce se viene eseguito da un utente che non dispone dei privilegi di amministratore. Il registro dell'installazione dell'CA MDB segnerà l'errore *ORA-00942: tabella o visualizzazione non esistente*.

Ulteriori informazioni:

[Installazione dell'CA MDB](#) (a pagina 116)

Pianificazione dell'installazione <USDK>

Seguire le indicazioni riportate di seguito per la ricerca e la raccolta di informazioni utili per pianificare l'installazione e la configurazione di CA Service Desk Manager in modo corretto.

- **Autorizzazioni di accesso** - Completare i passaggi seguenti:
 - (Windows) Accedere come amministratore con autorizzazioni di amministratore complete.
 - (UNIX) Accedere come utente root con le autorizzazioni appropriate per l'account root.
- **Ricerca** - Completare i passaggi seguenti:
 - Leggere *sia* le Note di rilascio che il file Leggimi facoltativo (se disponibili). Non avviare l'installazione prima di aver letto e compreso tali informazioni.

Nota: è possibile reperire la versione più aggiornata delle Note di rilascio, contenente i requisiti di sistema e il file Leggimi facoltativo (se disponibile), all'indirizzo <http://ca.com/support>.
 - Verificare di disporre del supporto di installazione.

Nota: se il computer non dispone di un'unità appropriata per il supporto di installazione, copiare il contenuto del supporto nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per avviare un'installazione remota in rete, potrebbe inoltre essere necessario condividere un'unità o una cartella in rete, quindi connettersi in rete.

Importante Non utilizzare i DVD di installazione di CA Service Desk Manager in un sistema operativo Windows XP, poiché alcuni file di installazione non verranno individuati e l'installazione non verrà completata correttamente.
 - Consultare la matrice della certificazione per un elenco dei prodotti software di terze parti certificati per l'utilizzo con CA Service Desk Manager.

Nota: è possibile trovare la versione più recente della matrice di certificazione all'indirizzo <http://ca.com/support>.
 - Leggere informazioni e acquisire le nozioni di base sui componenti del prodotto.

- Acquisire familiarità con i diversi tipi di strategie di implementazione supportate dal prodotto. Per la valutazione della strategia di implementazione più appropriata per la propria organizzazione, tenere presenti la disponibilità di rete, la larghezza di banda utilizzabile e i tempi di risposta.
- Leggere le considerazioni sull'implementazione per ciascun componente da installare.
- **Directory principale di installazione** - Completare i passaggi seguenti:
 - Scegliere la directory principale in cui si desidera installare il prodotto. La directory principale predefinita per il prodotto è C:\Programmi\CA\Service Desk.
 - Scegliere la directory principale in cui si desidera installare i componenti condivisi utilizzati dal prodotto (ad esempio JRE (Java Runtime Environment) e Apache Tomcat). La directory principale predefinita per i componenti condivisi è C:\Programmi\CA\SC.
- **Database** - Decidere quale database (SQL Server oppure Oracle) si desidera utilizzare con CA Service Desk Manager e installarlo. Quindi completare i passaggi seguenti:
 - **SQL Server.** Abilitare TCP/IP nel computer in cui si desidera eseguire l'installazione e la configurazione.
- **Server primario, secondario e configurazione utente** - Completare i passaggi seguenti:
 - Per garantire la corretta configurazione del server primario e, facoltativamente, del server secondario al termine dell'installazione del prodotto, è necessario disporre delle informazioni seguenti:
 - Il nome DNS (Domain Name System, sistema di denominazione dei domini) del server primario e secondario.
 - Il nome o l'alias del server.
 - Il nome o gli alias del gestore oggetti con il quale si desidera stabilire una connessione.
 - Il nome o l'indirizzo IP del server secondario.

- La porta socket slump che dovrà essere utilizzata da tutti i gestori di CA Service Desk Manager per la comunicazione.
- La porta socket proctor che dovrà essere utilizzata dal server secondario come porta di ascolto per i messaggi provenienti dal server primario.
- Per garantire la corretta configurazione delle informazioni di account per l'amministrazione del prodotto al termine dell'installazione, è necessario disporre di nome utente e password con diritti limitati e privilegi.
- (UNIX e Linux) È necessario creare manualmente gli utenti con diritti limitati e privilegi. In Windows tali utenti vengono creati automaticamente durante la configurazione del prodotto, mentre in UNIX e Linux è necessario crearli manualmente.
- **Configurazione dell'interfaccia Web** - Completare i passaggi seguenti:
 - Per garantire la corretta configurazione dell'interfaccia Web al termine dell'installazione del prodotto, è necessario disporre delle informazioni seguenti:
 - Il nome host Web e il server Web.
 - (Solo per Windows NT) Il sito Web che dovrà essere utilizzato dal server di CA Service Desk Manager.
 - Il numero di porta Tomcat e il numero di porta socket per le richieste di arresto.
- **Browser e software antivirus** - Completare i passaggi seguenti:
 - (Firefox) Se si desidera, abilitare l'autenticazione Windows (sessione unica aziendale).
 - Disabilitare temporaneamente eventuale software antivirus, in quanto rallenta l'installazione. Accertarsi di abilitarlo nuovamente al termine dell'installazione.
- **Screen Painter Web** - Screen Painter Web viene installato automaticamente nel server primario quando si installa CA Service Desk Manager. È possibile installare Screen Painter Web in computer separati utilizzando il supporto di installazione.
- **Creazione del nome file** - CA Service Desk Manager richiede Creazione del nome file 8.3. Vedere la documentazione di supporto e della Guida per ulteriori informazioni su Creazione del nome file 8.3 e sulla voce di registro disable8dot3.

Ulteriori informazioni:

[Componenti server primari o secondari](#) (a pagina 17)

[Strategie di implementazione](#) (a pagina 112)

[Abilitazione dell'autenticazione Windows in Firefox](#) (a pagina 113)

[Installazione di CA Service Desk Manager](#) (a pagina 122)

Considerazioni su USDK

Prima di installare CA Service Desk Manager, tenere presenti le informazioni seguenti per assicurarsi che l'implementazione venga eseguita correttamente:

- **Server Apache (UNIX e Linux)** - Se si utilizza il server Apache in UNIX o Linux, alcune installazioni di tale server disabilitano l'opzione FollowSymLinks nella directory principale. Tale opzione disabilita l'integrazione predefinita di Apache per CA Service Desk Manager, in quanto il file di configurazione utilizza il collegamento simbolico /opt/CAisd creato durante l'installazione di CA Service Desk Manager. Per consentire a CA Service Desk Manager di funzionare con Apache, è possibile abilitare FollowSymLinks dalla directory principale (operazione da eseguire nel file httpd.conf) oppure modificare il file \$NX_ROOT/bopcfg/www/CAisd_apache.conf per sostituire il collegamento simbolico con il percorso reale. Nel file CAisd_apache.conf cambiare tutte le occorrenze di /opt/CAisd con il percorso effettivo di USDK (ad esempio, /opt/CA/ServiceDesk). Dopo avere effettuato e salvato il cambiamento, arrestare e avviare il server Apache per applicare tale cambiamento.
- **Browser** - Tenere presenti le considerazioni seguenti:
 - (Firefox) Tenere presenti le considerazioni seguenti:
 - Potrebbe verificarsi un errore di "*Unprivileged Script*" quando si utilizzano le funzionalità Taglia/Copia/Incolla nella pagina di un editor HTML nelle categorie della conoscenza. Fare clic su OK per visualizzare una nota tecnica in mozilla.org, che mostra come consentire ad uno script di accedere agli appunti.
 - Quando si visualizza il contenuto di un file in allegato il cui nome contiene caratteri estesi Latin-1, viene visualizzata la finestra di dialogo popup Salva con nome. È possibile salvarlo su disco o fare clic per aprirlo e selezionare un'applicazione mediante la quale aprire l'allegato.
 - Se si sta utilizzando Internet Explorer 6 su Windows 2003 e il livello di Internet Security è impostato su Alto, è necessario aggiungere l'URL di CA Service Desk Manager e "*about:blank*" come Siti attendibili per le pagine Web per consentirne la corretta visualizzazione.

- Quando è in esecuzione la barra degli strumenti di Google, l'interfaccia Web di CA Service Desk Manager potrebbe presentare un problema durante la visualizzazione del testo della barra del titolo nella parte superiore della finestra.
- Se si sta utilizzando Internet Explorer 6.0 potrebbe verificarsi un periodico aumento dell'uso della memoria quando si accede all'interfaccia Web di CA Service Desk Manager. Si tratta di un problema noto dell'ultima release di Internet Explorer. Per rilasciare la memoria, ridurre periodicamente la pagina Web principale di CA Service Desk Manager.

■ **CA Workflow** - Tenere presenti le informazioni seguenti:

- Se durante la configurazione le credenziali dell'utente con privilegi non sono corrette, l'esecuzione di CA Service Desk Manager potrebbe riuscire ma sicuramente non riesce quella di CA Workflow. Se queste credenziali non sono corrette si potrebbe verificare ciò che segue:
 - CA Workflow non viene installato. Verrà citato un errore di nome utente/password non valido in /site/Workflow/wekinstall.log.
 - Tomcat richiede una quantità eccessiva di CPU, e/o il file di registro /log/pdm_tomcat_CAWF.log è stato riempito con eccezioni di gestione di sicurezza e messaggi "*AbandonedObjectPool è in uso*".

Per risolvere questa situazione, verificare la password e il nome utente con privilegi accedendo al sistema operativo con queste credenziali. Eseguire quindi la configurazione di CA Service Desk Manager e specificare password e nome utente con privilegi corretti. Se la password dell'utente con privilegi è stata cambiata, è necessario eseguire una configurazione per impostare la nuova password.

■ **Database (tutti supportati)** - Tenere presenti le informazioni seguenti:

- Se CA Service Desk Manager è stato configurato con un database, quindi la configurazione viene eseguita una seconda volta selezionando un tipo differente di database, la configurazione non funzionerà. Si supponga ad esempio di avere eseguito una configurazione iniziale per SQL Server e quindi di eseguire una nuova configurazione in un database Oracle. È necessario riavviare il computer prima di eseguire la seconda configurazione.
- Le informazioni per la connessione al database, se differenti, non sono accettate nelle configurazioni successive. Se occorre effettuare un'ulteriore configurazione come risultato del cambiamento nelle informazioni per la connessione al database, eliminare il file \$NX_ROOT\NX.env prima di procedere.

- Se è stato effettuato l'aggiornamento da Argis 8.0 a CA Asset Portfolio Management r11.2 e si condivide l'CA MDB (database) con CA Service Desk Manager, è possibile che si verifichino problemi nel tentativo di aggiungere o aggiornare gli asset nelle famiglie di asset mediante CA Service Desk Manager. Per evitare errori, è necessario definire le tabelle di estensione asset in CA Service Desk Manager servendosi di uno dei metodi seguenti:
 - Utilizzare Screen Painter Web per definire tabelle e moduli che consentono di visualizzare e modificare le voci della tabella.
 - Modificare manualmente le tabelle e i moduli mediante le linee guida seguenti:
 - a. Il file \$NX_ROOT\bopcfg\majic\assetx.maj contiene un modello che può essere usato per creare un file majic per identificare le colonne nella tabella di estensione asset in CA Service Desk Manager. Copiare il file e modificarlo come necessario seguendo le istruzioni che si trovano nel file.
 - b. Creare inoltre un file .sch nella directory \$NX_ROOT\site\mods per definire le colonne del database. I file \$NX_ROOT\site\assetx_schema.sch e \$NX_ROOT\site\assetx_index.sch possono essere usati come modelli che possono essere copiati e modificati appositamente per la tabella dell'estensione dell'attività.
- Nota:** è possibile creare il modulo per visualizzare i dati di estensione asset mediante Screen Painter Web.
- **SQL Server** - Tenere presenti le informazioni seguenti:
 - (SQL Server 2005) In SQL Server 2005 le credenziali password dell'utente sono più severe rispetto alle versioni precedenti di SQL Server. Assicurarsi che la password del database di CA Service Desk Manager coincida con le norme password definite in SQL Server. Se la password del database di CA Service Desk Manager non soddisfa le norme password di SQL Server 2005, sarà impossibile eseguire la configurazione di CA Service Desk Manager.
 - (Ambiente cluster Microsoft in SQL Server 2005) All'interno del cluster è necessario creare un alias per il nome del nodo virtuale SQL in modo da consentire la connessione di CA Service Desk Manager allo stesso nome server in caso di failover del cluster, indipendentemente dal nodo cluster attivo.

■ **Oracle** - Tenere presenti le informazioni seguenti:

- Se si installa CA Service Desk Manager in un sistema basato su UNIX con un database Oracle, è necessario che l'utente con privilegi appartenga al gruppo specificato durante l'installazione di Oracle. È possibile trovare il gruppo di installazione Oracle nel file denominato *oraInst.loc*.
- Durante la configurazione in un database Oracle a 64 bit in un computer a 64 bit, il percorso della libreria di sistema (LD_LIBRARY_PATH su Solaris, SHLIB_PATH su HP-UX e LIBPATH su AIX) deve indicare le librerie Oracle a 32 bit. Le librerie Oracle a 32 bit si trovano in \$ORACLE_HOME/lib32. Questo vale sia per la configurazione che per il runtime.
- Se si utilizza un database Oracle e si desidera utilizzare spazi tabelle esistenti, è necessario creare uno spazio tabelle Dati di almeno 400 MB, oltre ad uno spazio tabelle Indice di almeno 100 MB prima di configurare CA Service Desk Manager.

■ **Unità collegate esternamente** - Quando si installa CA Service Desk Manager in Linux con 20 o più unità collegate esternamente, potrebbe verificarsi un ritardo durante l'installazione dopo la visualizzazione delle pagine dell'installazione guidata e prima che venga visualizzata la pagina dello stato di avanzamento dell'installazione. Questo comportamento è normale e l'installazione dovrebbe riprendere.

■ **Install Shield e InstallAnywhere** - Tenere presenti le informazioni seguenti:

- Se si riceve un errore InstallShield quando si prova ad installare CA Service Desk Manager, attendere l'arresto dell'esecuzione di *msiexec.exe*. Provare ad installare il prodotto.
- Se si avvia, quindi si arresta l'installazione di CA Service Desk Manager in UNIX o Linux, è possibile che venga visualizzata una directory nella cartella principale dell'installazione denominata *install.dir.#####*. Si tratta di una funzionalità di InstallAnywhere. Tali file non sono necessari ed è possibile eliminarli senza problemi.

- **Directory principale di installazione** - Durante l'installazione di CA Service Desk Manager, non installare i componenti CA condivisi nella stessa directory dell'installazione di CA Service Desk Manager (NX_ROOT).
- **Internazionale** - Tenere presenti le informazioni seguenti:
 - Non è possibile utilizzare caratteri multi-byte sia per l'utente con il quale si è effettuato l'accesso sia per il nome utente CA Service Desk Manager con privilegi quando si esegue l'installazione in sistemi operativi multi-byte come cinese semplificato e giapponese. L'uso di tali caratteri rende impossibile l'installazione.
 - Non specificare caratteri multi-byte in nomi di percorsi file durante l'installazione e la configurazione. L'uso di tali caratteri rende impossibile l'installazione, la configurazione o entrambe.
 - È necessario che CA Service Desk Manager venga eseguito con le impostazioni internazionali UTF-8 sulle piattaforme Linux e UNIX.
 - I nomi Simbolo periodo forniti con l'installazione di CA Service Desk Manager predefinita (scheda Amministrazione, Service Desk, Dati applicazioni, Codici, Periodi) sono in inglese. Ad esempio, TODAY, YESTERDAY, THIS MONTH, e così via. Per quanto riguarda le versioni localizzate del prodotto, gli amministratori possono definire i nuovi Periodi localizzati come richiesto. È consigliabile non eliminare o modificare i Periodi predefiniti.
 - I formati di data in CA Service Desk Manager non supportano specificatori internazionali come gli specificatori di date localizzate (ad esempio, "jj/MM/AAAA" per il francese). La sintassi è limitata a specificatori generali, come "GG/MM/AAAA". Tuttavia, molti schemi schemi internazionali di date possono essere costruiti da questi specificatori generici (ad esempio, "AAAA.MM.GG" fornisce un formato di data giapponese comune).
 - Per notifiche di messaggi di posta elettronica in uscita come testo normale, le opzioni NX_SMTP_HEADER_CHARSET e NX_SMTP_BODY_CHARSET devono essere adattate (direttamente nel file NX.env) in modo da contrassegnare correttamente il messaggio di posta elettronica con il carattere codificato usato dall'ambiente operativo internazionale, affinché possa essere correttamente interpretato e visualizzato dai sistemi di posta elettronica del destinatario. I valori predefiniti per queste opzioni sono impostati su UTF-8 in tutte le piattaforme.

- Per le installazioni Oracle non in inglese in esecuzione su UNIX o Linux, è necessario impostare la variabile di ambiente NLS_LANG prima di eseguire pdm_init. Il DBA per Oracle dovrebbe verificare la documentazione Oracle relativa alle assegnazioni di valore per NLS_LANG.

Importante se non si imposta NLS_LANG, il client Oracle viene configurato per impostazione predefinita su *American_America.US7ASCII*. Ad esempio, per testare il giapponese multi-byte nel proprio ambiente, impostare NLS_LANG su *JAPANESE_JAPAN.UTF8*.

Nota: la variabile NLS_LANG deve essere impostata nella stessa shell prima dell'esecuzione di pdm_init. Ad esempio, *setenv NLS_LANG GERMAN_GERMANY.WE8ISO8859P1*

- Gli utenti internazionali possono adattare la proprietà del file web.cfg FormatoData in modo che vengano utilizzati i formati di data e data-ora più appropriati per la propria regione.
- Gli utenti internazionali possono modificare le impostazioni del controllo ortografico predefinite (l'opzione LEX_LANG in Gestione opzioni) con un dizionario che corrisponda alla lingua utilizzata nella propria regione.
- Dopo l'aggiornamento, gli ambienti operativi cinesi, giapponesi e coreani devono utilizzare il motore del modulo di ricerca FAST ESP.
- La versione inglese del server di CA Service Desk Manager è autenticata per operare in nove ambienti operativi non in lingua inglese. Per Windows, questi ambienti devono essere completamente localizzati nelle versioni internazionali dei sistemi operativi supportati dal Windows Server. In particolare, i sistemi operativi di Windows che utilizzano Language Interface Pack o MUI eseguiti su una base inglese non sono supportati.

Inoltre, versioni localizzate di CA Service Desk Manager sono supportate esclusivamente sui corrispondenti ambienti operativi di server Windows localizzati. In tutti i casi, è necessario che "Lingue per programmi non-Unicode" (tabella codici del sistema ANSI di Windows predefinita) del sistema sia configurato correttamente in Opzioni internazionali e della lingua nel Pannello di Controllo in modo da supportare la lingua di destinazione autenticata.

Nota: per ulteriori informazioni sulle versioni localizzate dei sistemi operativi Windows Server, consultare l'elenco Localized Microsoft Operating Systems su Microsoft's Global Development and Computing Portal.

- Le ricerche della conoscenza con caratteri giapponesi multi-byte per gli utenti internazionali di CA Service Desk Manager e Gestione delle informazioni funzioneranno correttamente con SQL Server solo se SQL Server è installato con la fascicolazione Windows. Assicurarsi di specificare l'opzione Fascicolazione dei dati durante l'installazione di SQL Server.

- **IPV4** - Quando si esegue l'installazione su piattaforme Linux, il file `/etc/hosts` deve contenere una voce IPV4 con l'indirizzo IP, il nome del computer e il nome completo del computer. Di seguito viene presentata una voce di esempio simile a quella indicata:

```
127.0.0.1 localhost.localdomain localhost
141.202.211.11 usbegp11.ca.com usbegp11
```

- **Nomi di file brevi** - Se sono stati disabilitati i nomi di file brevi sul sistema operativo Windows, è necessario abilitarli prima di installare CA Service Desk Manager. Inoltre, per abilitare i nomi di file brevi, è necessario impostare anche le variabili di ambiente TEMP e TMP su un nome di file breve, ad esempio, `c:\temp`, dopo l'abilitazione dei nomi di file brevi e prima di avviare il processo di installazione.

Nota: per informazioni, consultare l'articolo n. 121007 della Microsoft Knowledge Base nel sito Web Guida in linea e supporto tecnico Microsoft.

- **Caratteri speciali e spazi (nome cartella, percorso e directory)** -

Tenere presenti le informazioni seguenti:

- (UNIX e Linux) Se si copia il supporto di installazione su un disco rigido locale, assicurarsi che il percorso della directory di destinazione non contenga spazi o caratteri speciali (ad esempio `#`). In caso contrario, non sarà possibile eseguire l'installazione.
- (UNIX, Linux e Windows) *Non* inserire spazi nel percorso del supporto di installazione e nel nome della cartella. In caso contrario, non sarà possibile eseguire l'installazione.

- **Tomcat** - Tenere presenti le informazioni seguenti:

- Tomcat viene impostato come server Web predefinito di CA Service Desk Manager durante l'installazione del prodotto. Se si desidera utilizzare IIS (in Windows) oppure Apache (in UNIX o Linux) come server Web predefinito, eseguire l'installazione e selezionare IIS oppure Apache quando richiesto. In alternativa, eseguire nuovamente la configurazione selezionando IIS o Apache.
- Se Tomcat è configurato mediante un'autenticazione esterna su un server primario, è necessario impostare un server secondario con un motore Web e un daemon Repository per consentire agli utenti non autenticati di usare gli allegati. Per l'installazione di Tomcat in un server secondario non è possibile utilizzare un'autenticazione esterna.

- L'installazione di <SDK> imposta la porta Tomcat su 8080. Altri prodotti CA, come CA Asset Portfolio Management o la suite di prodotti Erogazione dei servizi, configurano la porta Tomcat sul valore predefinito 8080. Se si installano più prodotti CA nello stesso server, assicurarsi di scegliere una porta diversa da 8080 per consentire il corretto funzionamento delle successive installazioni del prodotto CA. Per cambiare il numero di porta Tomcat per CA Service Desk Manager, installare il prodotto. In alternativa, se è già stato installato, eseguire nuovamente la configurazione del prodotto e, quando richiesto, specificare un numero di porta disponibile per Tomcat.
- Dopo un riavvio, è possibile che il processo CA Service Desk Manager Tomcat non venga avviato. In questo caso, arrestare e riavviare Tomcat con i comandi seguenti:

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

■ **Utenti e autenticazione** - Tenere presenti le informazioni seguenti:

- L'autenticazione utente non funziona se il sistema utilizza file ombra e nel caso in cui ci sia una x nel campo password del file /etc/passwd.
- Nei sistemi HP se la protezione è stata configurata in modo tale che le password di sistema vengano archiviate in /etc/shadow, (ad esempio in /etc/passwd al posto delle password viene archiviata una x), l'autenticazione utente di CA Service Desk Manager non verrà eseguita, per cui gli utenti non potranno accedere a CA Service Desk Manager.
- Le password specificate per l'utente privilegiato e l'utente con restrizioni devono essere conformi ai vincoli dei criteri di password imposti dal dominio di rete. Se non soddisfano i vincoli imposti dal dominio, la configurazione di CA Service Desk Manager non viene eseguita correttamente.

■ **Interfaccia Web e IIS (Internet Information Services)** - Per configurare l'interfaccia Web con IIS 7.0 in Windows 2008, è necessario installare i componenti di compatibilità metabase e CGI di IIS 7.0. È possibile aggiungere questi componenti utilizzando la sezione Ruoli di Server Manager mediante l'installazione dei moduli di IIS Management Compatibility.

■ **Screen Painter Web** - Tenere presenti le informazioni seguenti:

- Quando si installa Screen Painter Web come parte dell'installazione di CA Service Desk Manager, è necessario configurarlo in modo appropriato per consentirne il corretto funzionamento.
- Con un'anteprima di sessione Screen Painter Web nella modalità test, cercare i filtri ignorati sulle nuove tabelle che non sono state pubblicate.

Ulteriori informazioni:

[Installazione di CA Service Desk Manager](#) (a pagina 122)

Componenti CA CMDB

CA CMDB fornisce i seguenti componenti standard:

Interfaccia Web CA CMDB.

- Consente di definire e registrare relazioni e proprietà di elementi della configurazione.
- Supporta l'analisi della causa principale e di impatto modifica.

Visualizzatore CMDB

- Consente di visualizzare graficamente le relazioni degli elementi della configurazione.
- Supporta la funzione di pianificazione

Controllo delle versioni

- Visualizza la cronologia delle modifiche e le relazioni degli elementi della configurazione.
- Confronta istantanee e milestone a cui è assegnato un nome.

Common Asset Viewer

- Consente una vista comune degli attributi degli asset in più prodotti.
- Rappresenta il punto di partenza nei prodotti di supporto.

Riconciliazione elementi della configurazione

- Associa i dati di elementi di configurazione importati con quelli esistenti in CA CMDB.
- Prevede l'uso dell'API del registro asset.

Repository

- Fornisce un archivio dati per elementi della configurazione, relazioni, famiglie e così via.
- Esiste nel MDB.

Integrazione

- Fornisce l'integrazione predefinita standard con CA Service Desk, CA NSM, CA Asset Portfolio Management, CA EEM ed altri prodotti.

Segnalazione

Include i seguenti rapporti per elementi della configurazione

- Riepilogo
- Dettagli
- Elementi della configurazione modificati
- Famiglia elemento della configurazione
- Relazione elementi di configurazione
- Struttura relazioni

CA CMDB fornisce i seguenti componenti opzionali:

- Universal Federation Adapters supporta l'importazione di dati di terze parti in CA CMDB.
- SMS Adapter supporta l'importazione di dati SMS in CA CMDB.

Considerazioni sulla pianificazione di Automazione supporto

È possibile utilizzare le informazioni riportate di seguito per cercare e raccogliere informazioni che consentono di pianificare una corretta configurazione di Automazione supporto.

- Per informazioni sui requisiti per Automazione supporto leggere le Note di rilascio.
- **Server e rete** - Considerare le seguenti modalità server Automazione supporto supportate:
 - **Server principale** - In Automazione supporto viene utilizzato il server applicazioni principale. Il server offre comunicazioni basate su socket e su HTTP.
 - **Server proxy socket** - In Automazione supporto viene utilizzato un proxy socket allo stesso livello del server Web che consente di scaricare l'elaborazione della crittografia/decriptografia dal server principale e garantire il supporto della scalabilità nelle connessioni socket dirette.
 - **Server messaggio di routing** - In Automazione supporto la larghezza di banda elevata e il traffico imprevedibile vengono separati dal server applicazioni principale per supportare la scalabilità server e offrire un collegamento al routing di rete per la scalabilità geografica mediante connessioni di Controllo remoto.

- **Dimensioni server** - Considerare le variabili server seguenti:
 - **Caratteristiche di rete delle connessioni utente finale e analista**
 - Il carico del server è direttamente proporzionale ai dati del componente di routing dei messaggi. Una bassa larghezza di banda, un'elevata latenza e una grande perdita di pacchetti contribuiscono in modo significativo a ridurre il carico sul server. Quando le condizioni della rete sono ottimali (larghezza di banda elevata, bassa latenza, perdita di pacchetti ridotta), la velocità sul server è di gran lunga superiore. Il numero totale di accessi utente finale e analista concorrenti al minuto, inclusi gli accessi utente self-service, può determinare un notevole carico di lavoro sul server.
 - **Tipo di connessione** - Il numero di connessioni socket rispetto al numero di connessioni HTTP influisce sui server nel modo seguente:
 - Quando ci si connette prevalentemente mediante connessioni socket, il carico sui server è talmente ridotto che, supponendo l'utilizzo di hardware potente, l'applicazione è associata alla rete anziché alla CPU. L'hardware non limita il numero di connessioni concorrenti ma la rete può limitare le connessioni.
 - Quando ci si connette tramite HTTP, il carico sui server applicazioni e Web è maggiore e l'applicazione è associata alla CPU a meno che non venga scalata in modo significativo.
 - **Utilizzo di Controllo remoto** - Controllo remoto utilizza una larghezza di banda di rete significativa in modo continuativo a ogni esecuzione. Tutto il traffico instradato tra gli utenti finali e gli analisti attraversa il server. Il numero di connessioni concorrenti di Controllo remoto ha un ruolo significativo nelle valutazioni relative alle dimensioni.

Nota: Controllo remoto è l'unico strumento a larghezza di banda elevata incluso nel toolset Assistenza in tempo reale. Conversione e Automazione utilizzano una larghezza di banda ridotta. Screenshot e Trasferimento file possono utilizzare una larghezza di banda elevata per brevi periodi di tempo durante il trasferimento dei file.

Considerazioni sulla larghezza di banda e sulla rete di Automazione supporto

La quantità di larghezza di banda utilizzata sul computer dell'utente finale dipende dagli strumenti utilizzati, come descritto di seguito:

- Per le funzionalità di chat e automazione, la quantità di larghezza di banda necessaria è ridotta. Per il relativo supporto è sufficiente un modem per linea telefonica da 56 kbps o meno.
- Per la funzionalità Controllo remoto la quantità di larghezza di banda necessaria è maggiore. Controllo remoto di Assistenza in tempo reale si adatta automaticamente agli ambienti con una larghezza di banda inferiore riducendo la qualità dell'immagine e la frequenza di aggiornamento della sessione di controllo remoto.

La quantità di larghezza di banda dipende anche dal modello di connessione in uso. Sono disponibili due modelli di connessione:

- Connettività HTTP: da utilizzare quando l'utente finale è protetto da un firewall restrittivo che consente solo connessioni HTTP al server.
- Socket diretto SSL: da utilizzare quando l'utente finale si connette al server utilizzando una connessione sulla porta SSL 443.

Nel grafico seguente viene illustrata la larghezza di banda necessaria in base agli strumenti utilizzati.

Strumenti/Larghezza di banda	Conversazione/Automazione	Remote Control
< 3 KBps (connessione 28,8 kbps)	Molto rapido e reattivo	Lento
< 5 KBps (connessione < 56 kbps)	Molto rapido e reattivo	Adeguito con riduzione della qualità delle immagini
< 50 KBps (cavo/ADSL)	Molto rapido e reattivo	Molto rapido e reattivo
< 100 KBps (LAN)	Molto rapido e reattivo	Molto rapido e reattivo

Pianificazione dell'installazione di CA EEM e CA Workflow

Seguire le indicazioni riportate di seguito per la ricerca e la raccolta di informazioni utili per pianificare l'installazione e la configurazione di CA EEM e CA Workflow in modo corretto.

- **Ricerca** - Completare i passaggi seguenti:
 - Leggere la documentazione relativa a CA EEM e CA Workflow, inclusi le Note di rilascio e il file Leggimi facoltativo (se disponibili).
 - **Nota:** CA EEM non è un'opzione di configurazione in CA Service Desk Manager. CA EEM richiede un'installazione separata.
 - Provare a vedere se si dispone di un'installazione di CA EEM esistente utilizzabile con CA Workflow. In caso affermativo, *non* installare nuovamente CA EEM. Installare invece CA Workflow e fare riferimento all'installazione di CA EEM esistente.
 - Prendere nota della password di amministrazione CA EEM, che servirà durante l'installazione.

- **Variabile di sistema JAVA_HOME** - Installare Java Runtime Environment 1.5 e impostare JAVA_HOME come variabile di sistema. Se non si imposta questa variabile di sistema, viene richiesto di specificare il percorso per l'installazione di Java 1.5. L'installazione di Java 1.5 è disponibile nel supporto di installazione nel percorso seguente:

- (Windows) \winsrvr.cd1\CA_tps.nt\JRE_1_5
- (Linux) /lnxsrvr.cd1/ca_tps.lnx/JRE_1_5
- (Solaris) /solsrvr.cd1/ca_tps.sol/JRE_1_5
- (AIX) /aixsrvr.cd1/ca_tps.aix/JRE_1_5

Nota: per informazioni sull'impostazione delle variabili di sistema, consultare la documentazione relativa al sistema operativo in uso.

- **Installazione CA Workflow** - Completare i passaggi seguenti:
 - Prima di provare ad installare CA Workflow, verificare di avere installato sia CA Service Desk Manager che CA EEM. Non è possibile installare CA Workflow se questi prodotti non sono installati.
 - Il valore predefinito per il numero di porta Tomcat per CA Service Desk Manager è 8080, mentre per CA Workflow è 8090. Se questi numeri di porta sono già utilizzati da un altro prodotto, cambiare i numeri di porta per CA Service Desk Manager e CA Workflow per evitare conflitti.

- **CA EEM e AIX** - Se si intende installare CA EEM in AIX ed è stato configurato AIX per NIS (Network Information Service), aggiungere un utente denominato *dsa* prima di installare CA EEM e CA Service Desk Manager. In questo caso procedere come segue:

1. Creare un utente con l'ID utente *dsa*.
2. Impostare la directory principale di *dsa* su */opt/CA/eTrustDirectory/dxserver*. Se le directory non esistono, crearle manualmente.

Nota: questo passaggio è necessario solo per CA EEM release 8.3 e precedenti. La directory principale per CA EEM 8.4 è cambiata in */opt/CA/Directory/dxserver* e viene creata automaticamente durante l'installazione.

3. Rendere *dsa* proprietaria di */opt/CA/eTrustDirectory* e di tutte le sottodirectory. Per rendere *dsa* proprietaria, è possibile utilizzare un comando simile al seguente:

chown -R dsa /opt/CA/eTrustDirectory

4. Verificare che l'utente esista, la directory principale e la proprietà di */opt/CA/eTrustDirectory*.

Ulteriori informazioni:

[Considerazioni su CA Workflow](#) (a pagina 94)

[Installazione di CA EEM](#) (a pagina 138)

[Installazione di CA Workflow](#) (a pagina 142)

[Installazione di CA Workflow IDE standalone](#) (a pagina 145)

Considerazioni su CA EEM

Prima di installare CA EEM, tenere presenti le informazioni seguenti per assicurarsi che l'implementazione venga eseguita correttamente:

- **Archivio dati LDAP esterno** - Se CA EEM è configurato per l'utilizzo di un archivio dati LDAP esterno, è necessario creare l'utente con privilegi nella directory LDAP.

Nota: per ulteriori informazioni sulla configurazione del server LDAP esterno, consultare la *Guida all'amministrazione*.

- **AIX** - Se si intende installare CA EEM 8.4 o versione successiva in AIX, non è necessario JRE 1.6. È possibile eseguire lo script di installazione con uno switch di esempio, come indicato di seguito:

```
/aixsvr.cd1/ca_tps.aix/EEM/EEMServer.sh -javahome none
```

Ulteriori informazioni:

[Installazione di CA EEM](#) (a pagina 138)

Considerazioni su CA Workflow

Prima di installare CA Service Desk Manager, tenere presenti le informazioni seguenti per assicurarsi che l'implementazione venga eseguita correttamente:

- **AIX (server primario) e JRE (Java Runtime Environment)** - In AIX per il server primario CA Service Desk Manager installa la versione IBM di JRE nella directory SC. La funzionalità di crittografia in JRE è limitata ed è necessario aggiornarla per consentire la funzione di Autenticazione CA EEM e CA Workflow. È possibile scaricare funzioni complete della crittografia dal sito Web IBM. Scaricare IBM SDK Policy Files, noto anche come Unrestricted JCE Policy files for SDK 1.5.

Nel server *primario* completare i passaggi seguenti:

1. Arrestare CA Service Desk Manager.
2. Copiare la cartella JRE 1.5 seguente dal supporto di installazione in una cartella specificata:

/aixsrvr.cd1/ca_tps.aix/JRE_1_5/jre

L'utente CA Service Desk Manager con privilegi deve eseguire le autorizzazioni su questa cartella e sul relativo contenuto.

Nota: il percorso della cartella JRE in NX.env verrà specificato nel passaggio 4.

3. Sostituire i file JAR dei criteri nella directory lib/security utilizzando i file JAR dei criteri del sito Web IBM.
 - a. Passare al sito Web IBM all'indirizzo seguente:
<http://www.ibm.com/developerworks/java/jdk/security/50/>
 - b. Fare clic sul collegamento "IBM SDK Policy Files" e seguire le istruzioni per il download.
 - c. Installare i file JAR e sostituire i file JAR dei criteri nella directory lib/security.

4. Aggiungere la voce seguente a NX.env:

NX_JRE_INSTALL_DIR_CAWF=<cartella JRE 1.5>

Nota: sostituire *<cartella JRE 1.5>* con il percorso specificato precedentemente al passaggio 2. Ad esempio,

NX_JRE_INSTALL_DIR_CAWF=/opt/testDVD/aixsrvr.cd1/ca_tps.aix/JRE_1_5/jre

5. Riavviare i servizi CA Service Desk Manager.

A questo punto è possibile accedere a CA Workflow. Se necessario, utilizzare l'ambiente di progettazione CA Workflow (IDE) per caricare o importare manualmente gli attori e le definizioni del processo forniti da CA Service Desk Manager. Questi ultimi si trovano in \$NX_ROOT/data/workflow nel server primario.

- **Utente o password del database CA MDB** - Tenere presenti le informazioni seguenti:
 - Modificando l'utente o la password del database CA MDB dopo l'installazione iniziale di CA Service Desk Manager, è necessario riavviare l'installazione di CA Workflow in modo tale che quest'ultimo applichi i cambiamenti e possa comunicare con CA Service Desk Manager. Quando si esegue nuovamente l'installazione di CA Workflow, CA Service Desk Manager imposta automaticamente il nuovo nome utente o la nuova password per CA Workflow e *non* è possibile modificare i valori manualmente durante l'installazione di CA Workflow.

Nota: prima di installare CA Workflow in UNIX e Linux, è necessario impostare le variabili di ambiente di Oracle. Se la variabile ORACLE_HOME non è impostata, viene visualizzato un messaggio di errore quando si fa clic sul collegamento per l'installazione.

- Se si esegue la migrazione ad un nuovo database, è necessario eseguire l'[utilità di migrazione flusso di lavoro](#) (a pagina 98).
- **IPV6** - Se il server Linux è configurato per il supporto IPv6, potrebbe essere impossibile accedere a CA Workflow IDE. Per correggere questa situazione, modificare il file script ide.sh situato in \$NX_ROOT\site\Workflow\Client modificando la seconda riga, ossia: "VMARGS =" in: "VMARGS=-Djava.net.preferIPv4Stack=true". Salvare il file script e avviare nuovamente CA Workflow IDE.
- **Tomcat** - Tenere presenti le informazioni seguenti:
 - Se l'avvio di Tomcat viene eseguito con difficoltà e, di conseguenza, l'interfaccia Web e CA Workflow non sono disponibili, aumentare la memoria Tomcat.

Nota: per informazioni su come risolvere questa situazione, cercare l'articolo TEC418959 della Knowledge Base all'indirizzo <http://ca.com/support>.

- Durante l'installazione di CA Workflow, CA Service Desk Manager e CA EEM condividono un numero di porta separato per Tomcat. In caso di problemi con l'installazione di Tomcat o l'utilizzo di CA Workflow, [arrestare e riavviare](#) (a pagina 212) il servizio.
 - Se sono state installate e modificate le impostazioni predefinite per la porta Tomcat (8080) o l'utente/password con privilegi predefiniti (ServiceDesk/ServiceDesk), sarà necessario effettuare i seguenti cambiamenti alle definizioni/attori CA Workflow predefiniti per consentirne il corretto funzionamento.
1. Accedere a Workflow IDE.
 2. Completare i passaggi seguenti per modificare il Service Desk Web Service Actor predefinito:
 - a. Fare clic sulla scheda Attori.
 - b. Espandere la struttura Servizio Web.
 - c. Fare clic con il tasto destro del mouse sull'attore Unicenter_Service_Desk_Web_Service e selezionare Proprietà.
 - d. Selezionare e copiare il contenuto della voce WSDL URL.
 - e. Modificare il nome dell'attore e fare clic su OK.
 - f. Fare clic con il pulsante destro del mouse sulla struttura Servizio Web e scegliere "Aggiungi attore".
 - g. Nel campo Nome immettere Unicenter_Service_Desk_Web_Service.
 - h. Nella voce WSDL URL incollare il contenuto copiato precedentemente.
 - i. Modificare il numero di porta nell'URL in modo che corrisponda al numero di porta selezionato durante la configurazione Tomcat.
 - j. Fare clic su OK.

Ulteriori informazioni:

[Installazione di CA Workflow](#) (a pagina 142)

Utilità di migrazione flusso di lavoro

Lo strumento Migrazione dati flusso di lavoro consente di trasferire i dati da un database CA Workflow a un altro. Questa utilità può trasferire i dati da uno dei database supportati ad un altro, nonché nell'ultimo schema CA Workflow.

Lo strumento Migrazione dati flusso di lavoro viene fornito sia come GUI (Interfaccia utente di tipo grafico, Graphical User Interface) che come Bean.

- **GUI**—migration.jar
- **Bean**—datamover.jar

Nota: per eseguire questi comandi Java, è necessario decomprimere manualmente due file JAR (datamover.jar e migration.jar) ed estrarli nel percorso Java. Il file Migration.zip si trova nel supporto di installazione nella directory \winsrvr.cd1\CA_tps.nt\CAFLOW\Resources.

Esecuzione dell'utilità di migrazione dalla riga di comando

Lo strumento di migrazione viene fornito come bean in datamover.jar. È possibile eseguire lo strumento di migrazione dalla riga di comando.

Esecuzione dell'utilità di migrazione

```
java -cp <file jar driver> com.ca.workflow.util.DataMover <nome driver db di origine> <url db di origine>  
<nomeutente db di origine> <password db di origine> <nome driver db di destinazione> <url db di destinazione>  
<nomeutente db di destinazione> <password db di destinazione> <numero di voci in una transazione> [codici  
prodotto (separati da virgola)]--fetchsize=15 [opzioni]
```

Esempio

```
java -cp ijdbc.jar;datamover.jar com.ca.workflow.util.DataMover ca.ingres.jdbc.IngresDriver  
jdbc:ingres://155.35.26.105:EI77/mdb;cursor=readonly;auto=multi;group=workflow_admin_group root iloveca  
ca.ingres.jdbc.IngresDriver jdbc:ingres://tadra01-w2k3-  
v:EI77/mdb;cursor=readonly;auto=multi;group=workflow_admin_group tadra01 ca#33333 50 wekProductKey1 --  
clean-target --fetchsize=15
```

file jar driver

Identifica il file o i file del driver sia di destinazione sia fonte. Separare più file dei driver utilizzando punti e virgola (;).

nome driver db di origine

Identifica il driver del database fonte.

url db di origine

Identifica l'URL del database fonte.

nomeutente db di origine

Identifica l'utente del database fonte.

password db di origine

Identifica la password del database fonte.

nome driver db di destinazione

Identifica il driver del database di destinazione.

URL db di destinazione

Identifica l'URL del database di destinazione.

nomeutente db di destinazione

Identifica l'utente del database di destinazione.

password db di destinazione

Identifica la password del database di destinazione.

numero di voci in una transazione

Specifica il numero di voci da spostare in una transazione. Se il numero è troppo elevato, esiste una possibilità di sovraccarico del registro transazioni Ingres. La porta 50 è quella consigliata.

clean-target

Rimuove dal database di destinazione tutti i dati correlati ai codici di prodotto specificati prima di procedere con il trasferimento dei dati. Se non sono specificati codici di prodotto, rimuove tutti i dati dal database di destinazione prima di procedere con il trasferimento dei dati. Questa opzione può essere utilizzata per ripulire un database di destinazione nel caso di esecuzione non riuscita di una precedente migrazione.

fetchsize

Se è presente, l'opzione della riga di comando -fetchsize specifica il numero di righe da recuperare per volta in un set di risultati a scorrimento. Se non viene specificata, l'utilità utilizzerà l'opzione fetchsize predefinita del database di origine. In Ingres non è presente alcun valore predefinito per il numero di righe da recuperare per volta in un set di risultati a scorrimento. In questo caso, viene utilizzato il valore predefinito di 10 righe, se tale valore non è specificato come opzione della riga di comando.

codici prodotto

Specifica i codici prodotto per cui migrare i dati. Questo parametro è facoltativo. Se viene specificato, può essere un codice prodotto singolo oppure un elenco di più codici prodotto separati da virgola. Se il parametro dei codici prodotto è presente, l'utilità di migrazione eseguirà la migrazione solo dei dati del database di origine vincolato dai codici prodotto specificati. Se questo parametro viene omissso, verrà eseguita la migrazione di tutti i dati relativi al flusso di lavoro indipendentemente dal codice prodotto.

File di registro

Quando si trasferiscono i dati da una riga di comando, viene creato un file di registro.

File del driver

Tutti i file del driver devono trovarsi nella directory dello strumento di migrazione oppure è necessario specificare il percorso del file JAR del driver di database.

Esecuzione dell'utilità di migrazione dalla GUI

Per eseguire la migrazione dalla GUI

1. Immettere il comando seguente nella riga di comando:

```
java -cp datamover.jar;migration.jar -Dwflog="c:\wf.log" -Dtxlimit="0" com.ca.workflow.util.WFMigration
```

Viene visualizzata la finestra di dialogo Strumento migrazione dati flusso di lavoro.

2. Per le sezioni relative al database fonte e di destinazione, selezionare il tipo di database dal menu a discesa Tipo database.

I nomi dei driver e gli URL vengono aggiornati automaticamente. È possibile modificare tali valori predefiniti, se necessario.

- Per Ingres, utilizzare -ijjdbc.jar
- Per Oracle 10g, utilizzare ojdbc14.jar
- Per Oracle 11g, utilizzare ojdbc5.jar
- Per MS SQL 2000, utilizzare msutil.jar, msbase.jar, mssqlserver.jar
- Per MS SQL 2005, utilizzare sqljdbc.jar
- Per Sybase Adaptive Server Enterprise 12.5.4, utilizzare jconn3.jar
- Per Sybase Adaptive Server Enterprise 15.0, utilizzare jconn3.jar

Importante per un elenco dei database supportati per CA Service Desk Manager, vedere le *Note di rilascio*.

3. Completare i campi appropriati.
4. Fare clic su Avvia.

Viene avviata la migrazione dei dati. Durante la migrazione, lo stato viene aggiornato nella parte inferiore della finestra di dialogo.

Pianificazione dell'integrazione di CA IT PAM

CA IT PAM è un prodotto CA autonomo con caratteristiche per l'automazione e il tracciamento di attività di amministrazione hardware e software in ambienti IT aziendali. CA IT PAM consente l'automazione di attività e gestisce le interazioni con l'utente, quali approvazioni e notifiche per la conformità e la precisione all'interno di ambienti di produzione.

Per pianificare l'interazione di CA IT PAM, tenere presente quanto segue:

- L'installazione e la configurazione del prodotto CA IT PAM richiedono parecchio tempo.
- Valutare se CA IT PAM e CA Service Desk Manager possono coesistere su un singolo server quando l'architettura server supporta entrambi i prodotti. Se i componenti CA IT PAM o CA Service Desk Manager non possono coesistere sullo stesso server, installare ogni prodotto su un server distinto.
- Calcolare il tempo necessario per verificare che entrambi i prodotti siano installati e funzionino in modo indipendente.

Nota: per informazioni sui requisiti dei prodotti CA Service Desk Manager e CA IT PAM, consultare le *Note di rilascio* di *CA Service Desk Manager*. Per informazioni sulle piattaforme supportate in CA IT PAM, sui passaggi necessari e sulle opzioni per l'installazione, consultare la documentazione relativa all'installazione e alla configurazione di CA IT PAM.

Considerazioni sulla protezione

Oltre ai requisiti minimi indicati nelle Note di rilascio, tenere presente i consigli seguenti per l'installazione di CA IT PAM:

- Configurare CA IT PAM per l'utilizzo di CA EEM come server di autenticazione. In CA EEM non è necessario passare i nomi e le password utente in testo normale a scopo di autenticazione.
- Se si utilizza la multi-tenancy per CA IT PAM, è richiesta l'installazione di CA EEM.

Nota: per informazioni sull'implementazione della multi-tenancy con CA IT PAM, consultare la documentazione relativa all'installazione e alla configurazione di CA IT PAM.

- Se si utilizza la multi-tenancy per CA Service Desk Manager, è richiesta l'installazione di CA EEM.

Nota: se non si utilizza la multi-tenancy, la configurazione di CA EEM per CA Service Desk Manager è facoltativa.

- Configurare CA IT PAM per comunicare utilizzando la comunicazione sicura su HTTPS. Gli URL HTTPS utilizzano SSL/TLS per eliminare gli scambi di testo normale e per proteggere i dati proprietari e altri dati sensibili dalla divulgazione accidentale o sleale.

Nota: per informazioni sulla configurazione di CA IT PAM per usare HTTPS, vedere la documentazione di installazione e configurazione di CA IT PAM.

Modalità di impostazione delle comunicazioni SSL con CA IT PAM

Per motivi di sicurezza, è possibile che gli implementatori di CA IT PAM scelgano di installare o riconfigurare CA IT PAM in modo da richiedere comunicazioni SSL. In questo caso, le applicazioni integrate come CA Service Desk Manager richiedono un certificato del keystore di CA IT PAM per le comunicazioni.

Per impostare le comunicazioni SSL con CA IT PAM, effettuare le operazioni seguenti:

1. Configurare le opzioni di CA Service Desk Manager in modo da utilizzare l'indirizzo HTTPS di CA IT PAM.
2. Esportare il certificato del keystore di CA IT PAM in un file e copiarlo in CA Service Desk Manager.
3. Caricare il file del certificato in CA Service Desk Manager utilizzando l'utilità `pdm_keystore_mgr` di CA Service Desk Manager.
4. Se applicabile all'architettura CA Service Desk Manager, aggiornare i file di controllo delle versioni per distribuire il keystore di CA Service Desk Manager su tutti i server secondari.
5. Riavviare CA Service Desk Manager.

Modalità di attivazione delle comunicazioni quando CA IT PAM è abilitato a SSL

Quando CA IT PAM comunica con SSL, è necessario configurare i server CA Service Desk Manager primario e secondario per le comunicazioni con CA IT PAM.

Per attivare le comunicazioni quando CA IT PAM è abilitato a SSL, effettuare le operazioni seguenti:

1. Verificare di poter utilizzare CA IT PAM in un browser, senza avviare CA Service Desk Manager. Registrare l'URL di CA IT PAM e utilizzarlo come riferimento durante la configurazione delle opzioni del flusso di lavoro di CA IT PAM in Gestione opzioni.
2. Accedere a CA Service Desk Manager e installare o modificare le opzioni del flusso di lavoro di CA IT PAM in Gestione opzioni. Per ognuna delle opzioni seguenti, utilizzare la sintassi `https://server:8443` anziché `http://server:8080` per accedere all'applicazione CA IT PAM abilitata a SSL. Se, tuttavia, per l'installazione di CA IT PAM viene utilizzata un'altra porta anziché la porta 8443 SSL, specificare il numero di porta appropriato.

- `caextwf_endpoint`
- `caextwf_processdisplay_url`
- `caextwf_worklist_url`

Nota: se i valori non corrispondono ai valori di installazione effettivi di CA IT PAM, CA Service Desk Manager non potrà comunicare con CA IT PAM e si verificherà un errore di runtime. Verificare che i valori corrispondano ai valori di installazione effettivi di CA IT PAM perché è possibile che durante l'esecuzione del programma di installazione di CA IT PAM sia stata selezionata una porta differente anziché la porta 8443.

3. Sul server CA IT PAM individuare la voce KEYSTOREID nel file seguente:
`C:\Progra~1\ITPAM\server\c2o\config\OasisConfig.properties`
4. Copiare KEYSTOREID. Prepararsi a incollare il valore KEYSTOREID come password dopo aver immesso il comando `keytool`.
5. Sul server CA IT PAM immettere in un'unica riga il comando `keytool` seguente nella riga di comando:
`C:\Progra~1\calsc\jre1.6.0_00\bin\keytool.exe -keystore C:\Progra~1\ITPAM\server\c2o\config\c2okeystore -export -alias c2o-j -file itpam.cer`

L'utilità `keytool` richiede una password.

6. Incollare o digitare il valore KEYSTOREID come password.

L'utilità `keytool` utilizza il parametro finale (`-file itpam.cer`) per creare un file denominato *itpam.cer*. Il file *itpam.cer* contiene le informazioni sul certificato necessarie per le comunicazioni con CA Service Desk Manager.

7. Spostare il file *itpam.cer* in una delle posizioni seguenti sul server CA Service Desk Manager:
 - (Windows) %NX_ROOT%\bin
 - (UNIX) \$NX_ROOT/bin
8. Importare le informazioni sul certificato CA IT PAM in CA Service Desk Manager immettendo il comando seguente:
(Windows) `pdm_perl %NX_ROOT%\bin\pdm_keystore_mgr.pl -import %NX_ROOT%\bin\itpam.cer`
(UNIX) `pdm_perl $NX_ROOT/bin/pdm_keystore_mgr.pl -import $NX_ROOT/bin/itpam.cer`

Lo script *pdm_keystore_mgr.pl* genera il file keystore nelle posizioni seguenti:
 - (Windows) %NX_ROOT%\pdmconf\nx.keystore
 - (UNIX) \$NX_ROOT/pdmconf/nx.keystore
9. Se l'architettura di CA Service Desk Manager include server secondari, *nx.keystore* deve essere distribuito in tutti i server secondari di CA Service Desk Manager. Aprire il file *server_secondary.ver* da una delle posizioni seguenti:
 - (Windows) %NX_ROOT%\site\server_secondary.ver
 - (UNIX) \$NX_ROOT/site/server_secondary.ver
10. Modificare il file *server_secondary.ver* per il controllo delle versioni aggiungendo le informazioni seguenti:
[SSL_Keystore]
filename = "nx.keystore"
directory = "\$NX_ROOT/pdmconf"
component_type = "file"
O_mode = "RW"
g_mode = "RW"
w_mode = "RW"
file_ctl

Nota: per informazioni sulla gestione del controllo delle versioni, consultare la *Guida all'amministrazione*.
11. Riavviare CA Service Desk Manager.

Il server CA Service Desk Manager può comunicare con l'applicazione CA IT PAM abilitata a SSL.

Nota: per informazioni sulla configurazione delle opzioni del flusso di lavoro di CA IT PAM, consultare la *Guida in linea*.

Pianificazione dell'installazione di CA Business Intelligence

Seguire le indicazioni riportate di seguito per la ricerca e la raccolta di informazioni utili per pianificare l'installazione e la configurazione di CA Service Desk Manager in modo corretto.

■ **Ricerca** - Completare i passaggi seguenti:

- Leggere le Note di rilascio per conoscere i requisiti relativi a CA Business Intelligence.
- Leggere la documentazione relativa a CA Business Intelligence, inclusi le Note di rilascio e il file Leggimi facoltativo (se disponibili).

Nota: per un elenco dettagliato degli ambienti supportati e dei requisiti hardware, consultare le varie Piattaforme Supportate nel DVD CA Business Intelligence. Questi documenti includono requisiti specifici a livello di versione e di patch per server di applicazioni web, browser web e sistemi operativi.

■ **Directory principale di installazione** - Scegliere la directory principale in cui si desidera installare CA Business Intelligence. I percorsi predefiniti sono:

- Per i computer Windows a 32 bit:
C:\Programmi\CA\SC\CommonReporting3
- Per i computer x64: C:\Programmi X(86)\CA\SC\CommonReporting3

Se questa directory non esiste, crearla prima di avviare l'installazione.

- **Software antivirus** - Disabilitare temporaneamente qualsiasi software antivirus in esecuzione sul computer in cui si desidera installare CA Business Intelligence.
- **Supporto server applicazione** - L'integrazione di CA Service Desk Manager con CA Business Intelligence supporta solo Apache Tomcat come server applicazione CA Business Intelligence.

Importante L'installazione di CA Business Intelligence è limitata alle piattaforme Windows solo per CA Service Desk Manager r12.5. È tuttavia possibile integrare CA Business Intelligence con CA Service Desk Manager in tutti i sistemi operativi supportati.

Ulteriori informazioni:

[Considerazioni sulla segnalazione](#) (a pagina 106)

[Installazione di CA Business Intelligence](#) (a pagina 157)

[Modalità di configurazione di CA Business Intelligence](#) (a pagina 173)

[Integrazione di CA Business Intelligence con CA Service Desk Manager](#) (a pagina 182)

Considerazioni sulla segnalazione

Prima di installare CA Business Intelligence, tenere presente le seguenti informazioni per assicurarsi che l'implementazione venga eseguita correttamente.

- È possibile richiesta un'installazione di CA Business Intelligence r3.0 (BusinessObjects Enterprise Release 3) per visualizzare i report r12.5 inclusi in questa release.
- CA Business Intelligence r2.1 (BusinessObjects Enterprise Release 2) non è supportato.
- È possibile installare CA Business Intelligence r3.0 durante il processo di aggiornamento dalla release 12.1 alla 12.5.
- Il processo di installazione varia in base al tipo selezionato, ovvero personalizzata oppure nuova.
- Prima di eseguire l'installazione, sia nuova che personalizzata, è necessario definire le credenziali dell'account amministratore di BusinessObjects.
- È necessario installare il CMS (Configuration Management Server) sulla porta 6400 (impostazione predefinita). In caso contrario, si verificherà un errore nella configurazione di CA Business Intelligence durante l'installazione.
- Per poter utilizzare i report, gli utenti di CA Service Desk Manager devono essere aggiunti all'elenco Amministratori in CMS.
- È necessario completare alcuni passaggi di configurazione aggiuntivi se si desidera installare Apache Tomcat 5.5.25 da utilizzare come server delle applicazioni per Business Objects.
- Gli utenti di SAP Business Objects con un'installazione esistente di Business Objects possono installare e configurare CA Business Intelligence (consigliato) oppure possono utilizzare l'installazione esistente di Business Objects.
- Se si intende accedere ad InfoView con Firefox, è necessario utilizzare la versione supportata di Firefox.
- Potrebbe essere necessario modificare la versione di JRE fornita con Business Objects in una versione più adatta all'ambiente specifico.
- Esplora risorse di Crystal Reports e Desktop Intelligence *non* sono supportati anche se possono essere richiamati dopo l'installazione di CA Business Intelligence.

Installazione nuova e personalizzata (Windows)

Esistono diverse differenze tra una nuova installazione e un'installazione personalizzata. In base al tipo selezionato, l'intero processo di installazione sarà diverso.

Nuovo

Installa tutti i componenti in un unico computer. Selezionare questo tipo di installazione per configurare velocemente una distribuzione completa, con tutti i componenti server e client in un unico computer. Una nuova installazione comporta:

- MySQL come database per memorizzare le informazioni di CMS.
- Apache Tomcat come server applicazioni

Nota: BusinessObjects Enterprise richiede un database per archiviare le informazioni su utenti e gruppi, livelli di protezione, contenuto BusinessObjects Enterprise e server. Il database primario, gestito da CMS, è noto come database CMS. Nel corso dell'installazione di CA Business Intelligence, si indica il CMS da utilizzare e si immettono i parametri necessari per l'autenticazione. Per ulteriori informazioni sui requisiti e sulla preparazione del database CMS, consultare la *Guida all'implementazione di CA Business Intelligence*.

Personalizzata

Installa i componenti selezionati nel computer. Selezionare questo tipo di installazione per specificare i componenti da installare quando si esegue una distribuzione ripartita oppure quando si aggiungono server ad una distribuzione esistente.

Importante Eseguire un'installazione personalizzata per installare il database CMS BusinessObjects in un database Microsoft SQL o in un database Oracle.

Un'installazione personalizzata consente di:

Installare MySQL o utilizzare un CMS già esistente, ovvero:

- Oracle
- Microsoft SQL
- Apache Tomcat - È possibile controllare l'installazione dell'istanza di Apache Tomcat.

Credenziali dell'amministratore di BusinessObjects

Prima di eseguire l'installazione, sia nuova che personalizzata, è necessario conoscere la password di amministratore di BusinessObjects.

Questa password deve essere composta da almeno sei caratteri, sia minuscoli che maiuscoli, e non può contenere la parola amministratore o eventuali varianti. La password deve inoltre contenere almeno due dei tipi di carattere seguenti:

- Maiuscolo
- Minuscolo
- Numerico
- Segno di punteggiatura

Server applicazioni BusinessObjects Enterprise XI

Affinché BusinessObjects Enterprise possa elaborare gli script su server per le applicazioni Web, è necessario disporre di un server applicazioni.

Durante l'installazione di CA Business Intelligence, specificare il server applicazioni da utilizzare e immettere i parametri di configurazione richiesti. CA Business Intelligence offre l'opportunità di installare Apache Tomcat 5.0.27. In alternativa, è possibile utilizzare il server applicazioni esistente.

Se si desidera installare Apache Tomcat 5.5.25 per utilizzarlo come server applicazioni per BusinessObjects, effettuare le operazioni seguenti:

- Installare Java 2 Standard Edition JDK 1.5.
- Impostare la variabile di ambiente \$JAVA_HOME nella directory principale di JDK 1.5.
- Installare Apache Tomcat 5.5.25 e impostare il percorso di Java Virtual Machine nella directory in cui è installato Java 2 Standard Edition JRE 1.6 nel sistema in uso.
- Completare un'installazione personalizzata di CA Business Intelligence.
- Nella schermata di configurazione del server Web selezionare "No" quando viene richiesto di installare una nuova copia di Tomcat per BusinessObjects XI.
- Selezionare Tomcat nell'elenco dei server applicazioni.
- Immettere il percorso del server Web Apache Tomcat 5.5.25 nel campo Directory di installazione e completare l'installazione.
- Dopo aver completato l'installazione di CA Business Intelligence, eseguire la configurazione di CA Business Intelligence.

Nota: se è già stato installato CA Business Intelligence con JDK 1.5 (mediante un server applicazioni esterno non predefinito) e si desidera utilizzare JRE 1.6 in un ambiente client che accede allo strumento Web Intelligence InfoView, non installare JRE 1.4.2 quando viene richiesto. Installare invece JRE 1.6 nell'ambiente client. Se possibile, riavviare il browser dopo avere installato JRE 1.6. È possibile scaricare JRE 1.6 da http://java.sun.com/javase/downloads/index_jdk5.jsp (download di Java Runtime Environment).

Installazione esistente di BusinessObjects (SAP)

Agli utenti di SAP BusinessObjects che dispongono di un'installazione esistente di BusinessObjects, non installata mediante CA Business Intelligence, si consiglia di installare e configurare CA Business Intelligence per garantire il livello massimo di compatibilità e supportabilità. Se si preferisce utilizzare l'installazione esistente di BusinessObjects, tuttavia, è possibile ignorare i passaggi di installazione di CA Business Intelligence e procedere con la sezione [Modalità di configurazione di CA Business Intelligence](#) (a pagina 173).

Nota: è necessario utilizzare BusinessObjects Enterprise release 3 ed aver distribuito Tomcat come server applicazioni. È inoltre necessario disporre della licenza per Web Intelligence. Per quanto riguarda Crystal Reports, è necessario disporre di una licenza runtime o superiore.

Accesso a InfoView con Firefox

Se si ha intenzione di accedere a BusinessObjects InfoView con Firefox, è necessario utilizzare Firefox 2 con Java Virtual Machine (Java Runtime) 1.5.0_xx e 1.6.0_02+.

Nota: per ulteriori informazioni sulle piattaforme supportate e sui livelli di release, consultare la *BusinessObjects Enterprise XI Release 2 SP4 for Windows Guide*.

Procedure ottimali del reporting

Utilizzare le procedure ottimali seguenti durante l'installazione, la gestione e l'utilizzo di CA Business Intelligence:

- Installare e gestire un universo per ogni prodotto CA. Se necessario, è possibile creare universi collegati.
- Prima di applicare service pack, patch e altri aggiornamenti al proprio universo personalizzato, eseguire il backup di tutte le personalizzazioni.
- Non modificare l'universo predefinito, ma copiarlo e modificarne la copia. In caso contrario, le personalizzazioni potrebbe essere cancellate in seguito all'applicazione di service pack, patch e altri aggiornamenti.
- Creare le cartelle personali.
- Se l'esecuzione dei report viene interrotta, verificare che il server CMS (Central Management Server) sia in esecuzione.
- Non sovrascrivere i report predefiniti.
- Utilizzare sempre un report predefinito come base per la creazione di un report personalizzato. In questo modo sarà possibile garantire la formattazione coerente di tutti i report.

Nota: per informazioni dettagliate sul completamento di queste attività, consultare la documentazione relativa a BusinessObjects Enterprise.

Pianificazione dell'installazione di CA NSM

Seguire le indicazioni riportate di seguito per la ricerca e la raccolta di informazioni utili per pianificare l'installazione e la configurazione di CA NSM in modo corretto.

- **Ricerca** - Completare i passaggi seguenti:
 - Leggere la documentazione relativa a CA NSM, inclusi le Note di rilascio e il file Leggimi facoltativo (se disponibili).
 - Verificare che CA NSM sia installato e configurato correttamente.

Ulteriori informazioni:

[Installazione dell'integrazione di CA NSM](#) (a pagina 137)

Pianificazione dell'installazione di FAST ESP

Seguire le indicazioni riportate di seguito per la ricerca e la raccolta di informazioni utili per pianificare l'installazione e la configurazione di FAST ESP in modo corretto.

■ **Ricerca** - Completare i passaggi seguenti:

- Leggere le *Note di rilascio* e *FAST ESP Installation Guide* per comprendere i requisiti di installazione, come hardware supportato, sistemi operativi e relative combinazioni, in aggiunta alle funzionalità di ricerca predefinite per il motore del modulo di ricerca FAST ESP.

Importante esiste un problema noto quando si installa FAST ESP in un server dove è stata abilitata l'opzione relativa all'ora legale. Per ulteriori informazioni, vedere le *Note di rilascio*.

- Leggere la documentazione di FAST ESP per acquisire familiarità con il motore del modulo di ricerca FAST ESP, apprendere come configurarlo e distribuirlo per prestazioni ottimali delle query e come proteggere il motore in modo adeguato. La guida all'installazione relativa a FAST ESP viene fornita nei supporti di installazione di CA Service Desk Manager.

■ **Directory principale di installazione** - Scegliere la directory principale in cui si desidera installare FAST ESP. Per impostazione predefinita, la directory principale per l'installazione di FAST ESP è C:\FastESP (Windows) e /opt/FastESP (Linux).

■ **Dopo l'installazione** - Configurare Gestione delle informazioni per l'utilizzo del motore di ricerca FAST ESP.

Nota: per ulteriori informazioni, consultare la *Guida all'amministrazione*.

Importante Non sarà possibile installare FAST ESP correttamente se nel server sono presenti tracce di un'installazione FAST ESP precedente o corrente. Chiudere tutti i processi FAST ESP e disinstallare il prodotto prima di provare ad installare FAST ESP.

■ **Configurazione utente e server** - Completare i passaggi seguenti:

- Tenere a portata di mano il nome di dominio completo o l'indirizzo IP (consigliato) del server dedicato in cui si installa FAST ESP.

Importante il server deve avere un indirizzo IP statico. Se il server non ha un indirizzo IP statico, non continuare con l'installazione. Riconfigurare il server con un indirizzo IP statico, quindi continuare con l'installazione.

- Scegliere un nome utente e una password per l'amministrazione della protezione di FAST ESP. Tale utente viene aggiunto al gruppo amministrativo ed è dotato di una protezione speciale per accedere come servizio.

Importante quando si accede a FAST ESP per la prima volta, è necessario utilizzare il nome utente "admin" senza password. Dopo questo accesso iniziale, è possibile creare utenti, gruppi e cambiare la password utente predefinita. Per ulteriori informazioni sull'accesso iniziale a FAST ESP, vedere *FAST ESP Home Guide*.

- (Linux) Creare l'utente FAST ESP. In Windows questo utente viene creato automaticamente durante l'installazione di FAST ESP, mentre in Linux è necessario crearlo manualmente.

Importante l'utente FAST è solo un utente locale, *non* un utente di dominio.

- Le ricerche in repository esterni funzionano solo quando la raccolta si chiama *sito*. Anche una raccolta già disponibile non può essere utilizzata se non si chiama *sito*. Ciò consente la corretta indicizzazione dei documenti.

Nota: per informazioni sulla creazione e sulla configurazione di raccolte, vedere *FAST ESP Configuration Guide*.

- Quando si imposta il limite delle dimensioni del testo degli allegati per ciascun documento, impostare il parametro max-index-size per i campi filetext e sul profilo di indice su un valore compreso tra 0 e 2GB. Il valore predefinito è 8196 KB.

Nota: per ulteriori informazioni sul parametro max-index-size, consultare il manuale *FAST ESP Configuration Guide*.

- **Software antivirus** - Disabilitare temporaneamente qualsiasi software antivirus in esecuzione sul computer in cui si desidera installare FAST ESP.

Ulteriori informazioni:

[Installazione di FAST ESP](#) (a pagina 153)

Strategie di implementazione

Quando si pianifica la strategia di implementazione CA Service Desk, tenere presenti, oltre alla disponibilità di rete, alla larghezza di banda utilizzabile e ai tempi di risposta, le considerazioni seguenti.

- **Centralizzata:** installa e configura tutti i componenti del prodotto nel server primario. Si tratta dell'installazione predefinita. È possibile implementare più gestori oggetti e motori Web per il bilanciamento del carico e il failover. Questa implementazione potrebbe tuttavia non essere sufficiente per le esigenze dell'azienda.

- **Distribuita:** installa e configura i componenti del prodotto nei server che si trovano in prossimità dei client che ricevono il servizio. È il caso, ad esempio, di una filiale di un'azienda dotata di una serie di subnet in cui possono esserci numerosi analisti che utilizzano il client Web. L'aggiunta di un server secondario in una filiale di questo tipo consente di ridurre il traffico di rete e i tempi di risposta. Viene inoltre ridotto il traffico di rete tra il server della filiale e il server primario, in quanto il server secondario esegue la memorizzazione nella cache. Questo tipo di implementazione supporta l'implementazione di più gestori oggetti e motori Web per il bilanciamento del carico e il failover.
- **Globale:** comprende due o più implementazioni centralizzate o distribuite definite regioni. Il server primario di una regione replica una quantità minima di informazioni in e da una regione principale. Ciò consente ad una regione di disporre di tutte le informazioni necessarie relative a tutte le altre regioni. Consente inoltre ad un analista di essere a conoscenza dei ticket di tutte le regioni ma di connettersi ad una regione solo se necessario. Questo tipo di implementazione risulta utile quando la larghezza di banda di rete è troppo limitata per un'implementazione distribuita. Ad esempio, è possibile che vi siano filiali dislocate in diversi paesi e connesse tra loro da un collegamento lento.

Abilitazione dell'autenticazione Windows in Firefox

L'autenticazione NT LAN Manager (NTLM) consente il trasferimento automatico delle credenziali di accesso per un utente Windows collegato ad un dominio Windows in un server Web IIS dello stesso dominio. Per impostazione predefinita, l'autenticazione Windows non è abilitata in Firefox. Per preparare l'implementazione, è necessario abilitare l'autenticazione Windows in Firefox.

Per abilitare l'autenticazione Windows in Firefox

1. Avviare Firefox.
2. Passare all'URL seguente:
about:config
3. Confermare che si desidera cambiare le impostazioni avanzate.
Viene visualizzato l'elenco Nome preferenza.
4. Individuare il nome preferenza *network.automatic-ntlm-auth.trusted-uris* e fare doppio clic su di esso:
Viene visualizzata la finestra di dialogo Inserire un valore stringa.

5. Specificare l'elenco dei siti attendibili immettendo l'URL completo (ad esempio, `http://web.example.com`) oppure il nome server (ad esempio, `web.example.com`)

Nota: non inserire la barra finale. Se si desidera specificare più server, separarli mediante una virgola. È possibile eseguire la corrispondenza di tutti i server di un dominio specifico ma generalmente i caratteri jolly non funzionano. Ad esempio, è necessario specificare `.example.com` anziché `*.example.com`.

6. Fare clic su OK.
7. Riavviare Firefox.

Capitolo 4: installazione

Questa sezione contiene i seguenti argomenti:

[Modalità di Implementazione del software](#) (a pagina 115)

[Installazione dell'CA MDB](#) (a pagina 116)

[Installazione di CA Service Desk Manager](#) (a pagina 122)

[L'installazione di Screen Painter Web](#) (a pagina 136)

[Installazione dell'integrazione di CA NSM](#) (a pagina 137)

[Installazione di CA EEM](#) (a pagina 138)

[Installazione di CA Workflow](#) (a pagina 142)

[Installazione di ADT](#) (a pagina 147)

[L'installazione di Federation Adapters di CA CMDB](#) (a pagina 148)

[Installazione di FAST ESP](#) (a pagina 153)

[Installazione di CA Business Intelligence](#) (a pagina 157)

[Verifica dell'installazione](#) (a pagina 163)

[Il registro di installazione](#) (a pagina 164)

Modalità di Implementazione del software

L'implementazione di CA Service Desk Manager dipende da diversi fattori, ad esempio dal sistema operativo in uso, dal database, dai prodotti che si desidera integrare, se si sta effettuando l'aggiornamento da una release precedente, se il prodotto viene installato per la prima volta e così via. In generale, seguire i passaggi seguenti per implementare il software:

1. Leggere le considerazioni sull'implementazione documentate nelle *Note di rilascio*.
2. Se si *effettua l'aggiornamento* da una versione precedente, seguire i passaggi per aggiornare il database, la console e CA Workflow.
3. Installare l'CA MDB.

Se il database (SQL Server o Oracle) è installato in un server diverso dal server CA Service Desk Manager primario, installare l'CA MDB nel server di database remoto (ovvero il computer in cui è installato SQL Server o Oracle). Se l'CA MDB e il server primario si trovano nello stesso computer, l'CA MDB viene installato automaticamente.

4. Installare CA Service Desk Manager nel server primario o nel server secondario facoltativo.

È possibile personalizzare i moduli web e lo schema dopo l'installazione in quanto Screen Painter Web viene installato automaticamente nel server.

5. (Facoltativo) Abilitare CA CMDB Visualizer durante la configurazione di CA Service Desk Manager.
6. (Facoltativo) Abilitare Automazione supporto durante la configurazione di CA Service Desk Manager.

Importante Se si desidera migrare le divisioni di CA Automazione supporto r6.0 SR1 eFix5 in titolari, convertire questi dati prima di abilitare e configurare Automazione supporto in CA Service Desk Manager r12.5.

7. (Facoltativo) Installare CA EEM per l'autenticazione.
8. (Facoltativo) Installare CA Workflow per gestire i processi aziendali.
9. (Facoltativo) Installare CA Business Intelligence per la gestione dei report con la tecnologia BusinessObjects.
10. (Facoltativo) Installare l'integrazione di CA NSM.
11. (Facoltativo) Installare il motore di ricerca FAST ESP da utilizzare con Gestione delle informazioni.

Ulteriori informazioni:

[Installazione dell'CA MDB](#) (a pagina 116)
[Installazione di CA Service Desk Manager](#) (a pagina 122)
[Installazione di CA EEM](#) (a pagina 138)
[Installazione di CA Workflow](#) (a pagina 142)
[Installazione di CA Business Intelligence](#) (a pagina 157)
[Installazione dell'integrazione di CA NSM](#) (a pagina 137)
[Installazione di FAST ESP](#) (a pagina 153)
[Verifica dell'installazione](#) (a pagina 163)
[Il registro di installazione](#) (a pagina 164)
[Avvio dell'interfaccia Web](#) (a pagina 172)

Installazione dell'CA MDB

Nota: prima di installare questo componente, verificare e leggere le informazioni su come pianificare un'installazione corretta.

Importante la mappatura dell'immagine DVD utilizzando un percorso UNC non è supportata per il programma di installazione di CA MDB.

Se il database (SQL Server o Oracle) che si desidera utilizzare con CA Service Desk Manager è installato in un server diverso dal server CA Service Desk Manager primario, installare manualmente l'CA MDB nel database remoto (ovvero, il computer in cui è installato SQL Server o Oracle). Se l'CA MDB e il server primario sono nello stesso computer, non è necessario completare questi passaggi. L'CA MDB viene installato automaticamente durante l'installazione di CA Service Desk Manager.

Nota: se si desidera installare il database di gestione nel server CA Service Desk Manager primario, è *necessario* avviare ed eseguire l'installazione dell'CA MDB sul computer remoto che ospita il server del database.

Ulteriori informazioni:

[Pianificazione dell'installazione <MDB>](#) (a pagina 74)

[Installazione in SQL Server \(Windows\)](#) (a pagina 118)

[Installazione in Oracle \(Windows\)](#) (a pagina 120)

[Installazione in Oracle \(Linux\UNIX\)](#) (a pagina 121)

Installazioni MDB

Per le installazioni MDB, vengono applicati i seguenti requisiti:

- Quando si esegue un'installazione MDB per installare il database SQL in un altro server, è necessario installare SQL Native Client, il client e gli strumenti di gestione SQL nel client CA CMDDB.
- Per la configurazione dei database Oracle, deve essere installato anche il software client di Oracle che è possibile scaricare dal sito Web di Oracle.

Ricerca dell'integrazione di prodotto e delle informazioni di compatibilità

È possibile utilizzare le informazioni fornite dal supporto in linea di CA per comprendere la compatibilità di CA MDB con CA Service Desk Manager e altri prodotti.

- *CA Service Accounting and CA Service Catalog Integration Guide*: vengono descritte le versioni di CA MDB e come stabilire se è necessario installare una patch per la compatibilità di CA MDB in modo da poter integrare altri prodotti in CA MDB.
- *CA Management Database Mixed Version Installation*: viene descritta la compatibilità di CA MDB.

Per trovare informazioni su CA MDB

1. Aprire un browser e andare all'indirizzo <http://support.ca.com>.
Verrà visualizzata la pagina del supporto in linea di CA.
2. Effettuare l'accesso al supporto in linea di CA.
3. Fare clic sul collegamento Documentation nel riquadro destro.
Viene visualizzata la pagina Documentation.

4. Selezionare CA Service Catalog, r12 e US English negli elenchi a discesa.
Fare clic su Vai.
Viene visualizzato l'elenco della documentazione CA Service Catalog.
5. Fare clic sul collegamento PDF per Integration Guide J02775-1E.
Viene visualizzata la guida *CA Service Accounting and CA Service Catalog Integration Guide*.
6. Fare clic sul segnalibro Enabling Integration with CA Products that Use an Earlier Version of the MDB.
È possibile utilizzare le informazioni per integrare i prodotti con CA MDB.

Per trovare informazioni sulla compatibilità

1. Aprire un browser e andare all'indirizzo <http://support.ca.com>.
Verrà visualizzata la pagina del supporto in linea di CA.
2. Effettuare l'accesso al supporto in linea di CA.
3. Fare clic su Knowledge Base Search nel riquadro Support.
Viene visualizzata la pagina Knowledge Base Search.
4. Immettere **MDB104 Compatibility** nel campo di ricerca. Fare clic su Ricerca.
Vengono visualizzati i risultati di Knowledge Base Search.
5. Fare clic su I collegamento CA Management Database Mixed Version Installation.
Viene visualizzato il documento *CA Management Database Mixed Version Installation*.

Installazione in SQL Server (Windows)

Se l'CA MDB utilizzato con CA Service Desk Manager si trova in un computer diverso rispetto al server CA Service Desk Manager, è *necessario* installare l'CA MDB nel *server di database remoto* (ovvero, nel computer in cui è installato SQL Server). Se l'CA MDB e il server primario sono nello stesso computer, non è necessario completare questi passaggi. Durante l'installazione di CA Service Desk Manager, l'CA MDB viene installato automaticamente.

Nota: non completare questi passaggi sul server CA Service Desk Manager primario. È *necessario* avviare ed eseguire l'installazione dell'CA MDB sul computer remoto che ospita il server del database.

Per installare l'CA MDB sul server del database remoto

1. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su CA MDB.
5. Per continuare con l'installazione, seguire le istruzioni visualizzate.
6. Alla richiesta, selezionare SQL Server come tipo di database e immettere le informazioni appropriate per SQL Server.

Nota: se non si è sicuri di quali informazioni immettere per SQL Server, vedere la *Guida in linea della configurazione del server*.

7. Continuare seguendo le istruzioni visualizzate per completare l'installazione dell'CA MDB.

L'CA MDB viene installato in Oracle.

Ulteriori informazioni:

[Il registro di installazione](#) (a pagina 164)

Installazione in Oracle (Windows)

Se l'CA MDB utilizzato con CA Service Desk Manager si trova in un computer diverso rispetto al server CA Service Desk Manager, è *necessario* installare l'CA MDB nel *server di database remoto* (ovvero, nel computer in cui è installato Oracle). Se l'CA MDB e il server primario sono nello stesso computer, non è necessario completare questi passaggi. Durante l'installazione di CA Service Desk Manager, l'CA MDB viene installato automaticamente.

Nota: non completare questi passaggi sul server CA Service Desk Manager primario. È *necessario* avviare ed eseguire l'installazione dell'CA MDB sul computer remoto che ospita il server del database.

Per installare l'CA MDB nel server del database remoto

1. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

2. Fare clic sulla scheda Installazione prodotto.
3. Fare clic su CA MDB.
4. Per continuare con l'installazione, seguire le istruzioni visualizzate.
5. Alla richiesta, selezionare Oracle come tipo di database e immettere le informazioni appropriate per Oracle.

Nota: se non si è certi di cosa immettere per Oracle, vedere la *Guida in linea della configurazione del server*.

6. Continuare seguendo le istruzioni visualizzate per completare l'installazione dell'CA MDB.

L'CA MDB viene installato in Oracle.

Ulteriori informazioni:

[Il registro di installazione](#) (a pagina 164)

Installazione in Oracle (Linux\UNIX)

Se l'CA MDB utilizzato con CA Service Desk Manager si trova in un computer diverso rispetto al server CA Service Desk Manager, è *necessario* installare l'CA MDB nel *server di database remoto* (ovvero, nel computer in cui è installato Oracle). Se l'CA MDB e il server primario sono nello stesso computer, non è necessario completare questi passaggi. Durante l'installazione di CA Service Desk Manager, l'CA MDB viene installato automaticamente.

Importante Non eseguire questi passaggi sul server CA Service Desk Manager primario. È *necessario* avviare ed eseguire l'installazione di CA MDB sul computer remoto che ospita il server del database.

Nota: verificare che il proprio ambiente Oracle sia configurato in modo corretto e che sia accessibile.

Per installare l'CA MDB nel server del database remoto

1. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Accedere alla directory principale del supporto di installazione e avviare l'installazione eseguendo il comando seguente:

```
sh ./setup.sh
```

3. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.
Viene visualizzato il menu di installazione.
4. Fare clic sulla scheda Installazione prodotto.
5. Fare clic su CA MDB.

6. Per continuare con l'installazione, seguire le istruzioni visualizzate.
7. Alla richiesta, selezionare Oracle come tipo di database e immettere le informazioni appropriate per Oracle.

Nota: se non si è certi di cosa immettere per Oracle, vedere la *Guida in linea della configurazione del server*.

8. Continuare seguendo le istruzioni visualizzate per completare l'installazione dell'CA MDB.

L'CA MDB viene installato in Oracle.

Ulteriori informazioni:

[Il registro di installazione](#) (a pagina 164)

Installazione di CA Service Desk Manager

Nota: prima di installare questo componente, leggere le informazioni su come pianificare un'installazione corretta. Quando si esegue l'installazione in Linux e UNIX, alcuni messaggi pop-up non vengono visualizzati chiaramente se le proprietà dei colori sono bianco su bianco.

Quando si avvia e si installa CA Service Desk Manager sul server primario o secondario, vengono installati i file, i componenti e le funzionalità seguenti:

- Funzionalità server primaria e secondaria, basata sulla modalità di configurazione del prodotto dopo l'installazione.
- L'interfaccia SQL Server oppure Oracle
- L'interfaccia ODBC

Importante l'installazione dell'interfaccia ODBC è destinata al solo utilizzo per accedere al driver ODBC per il reporting Business Objects in CA Service Desk Manager con CA Business Intelligence. L'utilizzo del driver ODBC da parte di altre applicazioni non è direttamente supportato, certificato o garantito da CA. Pertanto l'utilizzo è sotto la responsabilità dell'utente.

- L'interfaccia Web
- CA CMDB

Importante Durante la configurazione, quando viene eseguita la migrazione dalla versione autonoma di CA CMDB a CA Service Desk Manager, viene visualizzata la casella di controllo Configurazione solo CMDB. Se si deseleziona la casella di controllo Configurazione solo CMDB e si fa clic su Avanti, non è più possibile configurare CA CMDB. Anche se si sceglie Indietro, la casella di controllo Configurazione solo CMDB non è più disponibile. Un messaggio informa l'utente di questo comportamento nella finestra di dialogo della configurazione. Se si annulla la configurazione prima del termine e la si riesegue, la casella di controllo Configurazione solo CMDB è nuovamente disponibile.

La casella di controllo Configurazione solo CMDB controlla il valore della variabile di ambiente NX_CMDB di CA Service Desk Manager. La variabile di ambiente controlla se è configurata la funzione Automazione supporto. Se la casella di controllo è deselezionata, Automazione supporto è configurabile; in caso contrario, non lo è. La variabile di ambiente influisce sul comportamento di alcuni moduli Web.

- Visualizzatore
- Automazione supporto

L'opzione *supportautomation_url* deve essere installata dopo la configurazione di Automazione supporto durante la configurazione di CA Service Desk Manager. Per ulteriori informazioni, vedere la *Guida in linea*.

Importante quando si disinstalla CA Service Desk Manager, anche CA Workflow viene disinstallato.

Ulteriori informazioni:

[Pianificazione dell'installazione <USDK>](#) (a pagina 78)

[Installazione su SQL Server \(Windows\)](#) (a pagina 123)

[Installazione su Oracle \(Windows\)](#) (a pagina 125)

[Installazione su Oracle \(Linux\UNIX\)](#) (a pagina 129)

Installazione su SQL Server (Windows)

Quando si avvia e si installa CA Service Desk Manager sul server primario o secondario, vengono installati i componenti e le caratteristiche seguenti:

- Funzionalità server primaria e secondaria, basata sulla modalità di configurazione del prodotto dopo l'installazione.
- L'interfaccia di SQL Server
- L'interfaccia Web
- L'interfaccia ODBC

Importante l'installazione dell'interfaccia ODBC è destinata al solo utilizzo per accedere al driver ODBC per il reporting Business Objects in CA Service Desk Manager con CA Business Intelligence. L'utilizzo del driver ODBC da parte di altre applicazioni non è direttamente supportato, certificato o garantito da CA. Pertanto l'utilizzo è sotto la responsabilità dell'utente.

Per installare CA Service Desk Manager in SQL Server

1. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su CA Service Desk Manager.
5. Per continuare con l'installazione, seguire le istruzioni sullo schermo.

Viene visualizzata la Configurazione guidata.

Nota: se gli host protocollo Internet versione 4 (IPv4) e protocollo Internet versione 6 (IPv6) coesistono sulla rete, verificare che siano utilizzate le strategie, gli strumenti e i meccanismi di transizione appropriati per supportare tali tecnologie prima di avviare la configurazione del prodotto. Per informazioni sulla configurazione dei server, vedere la *Guida all'amministrazione*.

6. Immettere e selezionare le informazioni per configurare il prodotto.

Nota: per informazioni sui campi che compaiono nella creazione guidata, vedere la *Guida in linea*.

7. Continuare seguendo le istruzioni sullo schermo per completare l'installazione.
CA Service Desk Manager viene installato in SQL Server.
8. Una volta installato CA Service Desk Manager (o eseguita la migrazione su CA Service Desk Manager da un sistema autonomo CA CMDB), eseguire l'utilità *cmdb_update_ambiguity*. Utilizzare il comando -h per visualizzare le opzioni obbligatorie. Per ulteriori informazioni sul calcolo dell'indice di ambiguità, consultare la *Guida all'amministrazione*.

Nota: se durante il passaggio di validazione delle tabelle estensioni la configurazione non riesce, la connettività del database può essere un problema. Eseguire di nuovo la configurazione e verificare di aver specificato informazioni corrette sulla connettività del database.

Ulteriori informazioni:

[Il registro di installazione](#) (a pagina 164)

[Verifica dell'installazione](#) (a pagina 163)

[Avvio dell'interfaccia Web](#) (a pagina 172)

Installazione su Oracle (Windows)

Quando si avvia e si installa CA Service Desk Manager sul server primario o secondario, vengono installati i componenti e le caratteristiche seguenti:

- Funzionalità server primaria e secondaria, basata sulla modalità di configurazione del prodotto dopo l'installazione.
- L'interfaccia Oracle
- L'interfaccia Web
- L'interfaccia ODBC

Per installare CA MDB o CA Service Desk Manager è necessario essere amministratori.

Importante l'installazione dell'interfaccia ODBC è destinata al solo utilizzo per accedere al driver ODBC per il reporting Business Objects in CA Service Desk Manager con CA Business Intelligence. L'utilizzo del driver ODBC da parte di altre applicazioni non è direttamente supportato, certificato o garantito da CA. Pertanto l'utilizzo è sotto la responsabilità dell'utente.

Per installare CA Service Desk Manager su Oracle

1. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su CA Service Desk Manager.
5. Per continuare con l'installazione, seguire le istruzioni sullo schermo.

Viene visualizzata la Configurazione guidata.

Nota: se gli host protocollo Internet versione 4 (IPv4) e protocollo Internet versione 6 (IPv6) coesistono sulla rete, verificare che siano utilizzate le strategie, gli strumenti e i meccanismi di transizione appropriati per supportare tali tecnologie prima di avviare la configurazione del prodotto. Per informazioni sulla configurazione dei server, vedere la *Guida all'amministrazione*.

6. Immettere e selezionare le informazioni per configurare il database Oracle.

In CA Service Desk Manager è necessario specificare un nome del servizio di rete Oracle che indica il database Oracle in cui risiede l'MDB. Inoltre è necessario specificare un SID (identificatore di sistema) per il database. I nomi possono essere diversi, anche se specificano lo stesso database MDB. Per CA Service Desk Manager è necessario specificare due valori nome perché accede al database sia con la tecnologia client Oracle sia con la tecnologia JDBC.

Nota: per informazioni su nomi di servizi e sui SID, consultare la documentazione Oracle.

Carica dati predefiniti

Specifica se caricare i dati CA Service Desk Manager predefiniti nel database Oracle.

Se questa casella di controllo è selezionata, i dati del sistema predefinito di CA Service Desk Manager vengono caricati nel database Oracle. Se sono stati modificati eventuali valori predefiniti di sistema, questa opzione sostituisce i valori. Selezionare questa casella di controllo per le prime installazioni. L'uso di questa opzione determina la sostituzione dei dati esistenti nel caso in cui non si tratti di una prima installazione. Se la casella di controllo non è selezionata, non vengono caricati dati predefiniti.

Database remoto

Indica che un database Oracle viene installato in un server diverso dal server primario CA Service Desk Manager. Installare manualmente CA MDB nel server del database remoto, ovvero nel computer in cui è installato Oracle, prima di eseguire l'installazione di CA Service Desk Manager.

Se il server Oracle è locale (non selezionato), CA Service Desk Manager crea MDB se non è stato già creato.

Crea Spazi tabelle

Specifica se creare spazi tabelle per il database MDB o utilizzare spazi tabelle già creati.

- Deselezionare questa casella di controllo se sono stati già creati spazi tabelle manualmente. Fornire i nomi degli spazi tabelle esistenti. Il campo del percorso dello spazio tabelle nel prodotto è disabilitato mentre i campi Nome spazio tabelle dati e Nome spazio tabelle indice sono abilitati.
- Selezionare questa casella di controllo per creare spazi tabelle con i nomi predefiniti MDB_DATA e MDB_INDEX. Specificare un percorso dello spazio tabelle. I campi nome degli spazi tabelle Dati e Indice vengono disattivati.

Nota: se si utilizza Automated Storage Manager (ASM) di Oracle, creare manualmente uno spazio tabelle Oracle prima di eseguire l'installazione di CA Service Desk Manager. Quando Oracle è installato e configurato per ASM, non è possibile creare uno spazio tabelle Oracle durante l'installazione di MDB. ASM utilizza l'archiviazione virtuale. Si sta invece cercando una directory fisica. Non è pertanto possibile creare lo spazio tabelle con questa configurazione.

Nome servizio di rete

Identifica il Nome servizio di rete del database Oracle in cui risiede l'MDB. Se il database è remoto, utilizzare il nome servizio di rete definito nel client Oracle sul computer locale. CA Service Desk Manager accede al database utilizzando un'installazione locale del client Oracle, che potrebbe specificare un nome servizio di rete diverso dal nome del servizio sul server Oracle.

Password utente mdbadmin

Specifica la password utente mdbadmin. Fornire la password esistente o specificare una nuova password se CA Service Desk Manager crea l'utente.

Nome utente DBA

Specifica il nome di un utente Oracle con accesso DBA (in genere SYS). Questo campo viene utilizzato solo se il server Oracle si trova sul computer locale.

Password DBA

Identifica la password per l'utente DBA. Questo campo viene utilizzato solo se il server Oracle si trova sul computer locale.

Nome spazio tabelle dati

Crea il nome dello spazio tabelle dati specificato quando è selezionata la casella di controllo Crea spazio tabelle. Questo campo viene utilizzato solo se il server Oracle si trova sul computer locale.

Nome spazio tabelle indice

Crea il nome dello spazio tabelle indice specificato quando è selezionata la casella di controllo Crea spazio tabelle. Questo campo viene utilizzato solo se il server Oracle si trova sul computer locale.

Percorso spazio tabelle

Specifica il percorso fisico della directory dello spazio tabelle creato se gli spazi tabelle precedentemente menzionati non esistono. Questo campo viene utilizzato solo se il server Oracle si trova sul computer locale.

Percorso pagina principale Oracle

Specifica il percorso di directory della pagina principale Oracle.

Connettività JDBC

Specifica se utilizzare Connettività JDBC. Alcuni componenti di CA Service Desk Manager utilizzano la tecnologia JDBC per accedere al database e richiedono informazioni specifiche sul server Oracle.

Identificare la porta di ascolto, il SID e il nome host del database configurati in precedenza.

7. Continuare seguendo le istruzioni sullo schermo per completare l'installazione.
CA Service Desk Manager viene installato su Oracle.
8. Una volta installato CA Service Desk Manager (o eseguita la migrazione su CA Service Desk Manager da un sistema autonomo CA CMDB), eseguire l'utilità *cmdb_update_ambiguity*. Utilizzare il comando -h per visualizzare le opzioni obbligatorie. Per ulteriori informazioni sul calcolo dell'indice di ambiguità, consultare la *Guida all'amministrazione*.

Ulteriori informazioni:

[Il registro di installazione](#) (a pagina 164)

[Verifica dell'installazione](#) (a pagina 163)

[Avvio dell'interfaccia Web](#) (a pagina 172)

Installazione su Oracle (Linux\UNIX)

Quando si avvia e si installa CA Service Desk Manager sul server primario o secondario, vengono installati i componenti e le caratteristiche seguenti:

- Funzionalità server primaria e secondaria, basata sulla modalità di configurazione del prodotto dopo l'installazione.
- L'interfaccia Oracle
- L'interfaccia Web
- L'interfaccia ODBC

Importante l'installazione dell'interfaccia ODBC è destinata al solo utilizzo per accedere al driver ODBC per il reporting Business Objects in CA Service Desk Manager con CA Business Intelligence. L'utilizzo del driver ODBC da parte di altre applicazioni non è direttamente supportato, certificato o garantito da CA. Pertanto l'utilizzo è sotto la responsabilità dell'utente.

Nota: verificare che il proprio ambiente Oracle sia impostato in modo corretto e che sia accessibile.

Per installare CA Service Desk Manager su Oracle

1. Inserire il supporto di installazione sulla propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Accedere alla directory principale del supporto di installazione e avviare l'installazione eseguendo il comando seguente:

```
sh ./setup.sh
```

3. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: quando si esegue l'installazione in Linux e UNIX, è possibile che alcuni messaggi pop-up non vengano visualizzati in modo chiaro, se le proprietà dei colori sono bianco su bianco.

4. Fare clic sulla scheda Installazione prodotto.
5. Fare clic su CA Service Desk Manager.
6. Per continuare con l'installazione, seguire le istruzioni sullo schermo.

Viene visualizzata la Configurazione guidata.

Nota: se gli host protocollo Internet versione 4 (IPv4) e protocollo Internet versione 6 (IPv6) coesistono sulla rete, verificare che siano utilizzate le strategie, gli strumenti e i meccanismi di transizione appropriati per supportare tali tecnologie prima di avviare la configurazione del prodotto. Per informazioni sulla configurazione dei server, vedere la Guida all'amministrazione.

7. Immettere e selezionare le informazioni per configurare il prodotto.

Nota: per informazioni sui campi che compaiono nella creazione guidata, vedere la *Guida in linea*.

8. Continuare seguendo le istruzioni sullo schermo per completare l'installazione.

CA Service Desk Manager viene installato su Oracle.

9. Una volta installato CA Service Desk Manager (o eseguita la migrazione su CA Service Desk Manager da un sistema autonomo CA CMDB), eseguire l'utilità `cmdb_update_ambiguity`. Utilizzare il comando `-h` per visualizzare le opzioni obbligatorie. L'opzione `-d` non è richiesta in un ambiente Linux/Unix, in quanto l'impostazione predefinita è Oracle.

Nota: per ulteriori informazioni sul calcolo dell'indice di ambiguità, consultare la *Guida all'amministrazione*.

Ulteriori informazioni:

[Il registro di installazione](#) (a pagina 164)

[Verifica dell'installazione](#) (a pagina 163)

[Avvio dell'interfaccia Web](#) (a pagina 172)

Configurazione di Visualizer

È possibile configurare Visualizer durante l'installazione di CA Service Desk Manager. Quando si seleziona la casella di controllo Configurazione Visualizer, vengono visualizzati i pannelli per la configurazione di Visualizer.

Selezionando il pulsante Avanti della procedura guidata, si convalidano le informazioni sulla configurazione. Se la validazione viene completata correttamente, le informazioni sulla configurazione di Visualizer convalidate vengono utilizzate per l'attività di configurazione di Visualizer.

Modalità di configurazione di Visualizer in un server secondario

È possibile configurare Visualizer in un server CA Service Desk Manager secondario per l'utilizzo dei servizi Web. Avviare e configurare Visualizer in un server secondario durante la configurazione di CA Service Desk Manager utilizzando l'utilità *pdm_edit*.

Nota: se si esegue la configurazione per utilizzare i servizi Web secondari in un'installazione secondaria di CA CMDB Visualizer, selezionare il nome server dal menu di scelta rapida. Il server primario rappresenta la selezione predefinita.

Per configurare Visualizer in un server secondario

1. Selezionare Configurazione Visualizer nella pagina della configurazione guidata di Visualizer.
2. Selezionare il server CA Service Desk Manager secondario come host Web e specificarne la porta.

Se la configurazione è in esecuzione su un server CA Service Desk Manager secondario, è possibile utilizzare il menu di scelta rapida per scegliere i valori delle proprietà `general.primary_server_node` e `general.local_host` degli host dei servizi Web disponibili.

3. Immettere il numero di porta CA Service Desk Manager per il server Visualizer secondario.

4. Continuare seguendo le istruzioni sullo schermo per completare l'installazione.

Visualizer viene installato e configurato su un server CA Service Desk Manager secondario.

5. Aprire un prompt dei comandi e passare alla cartella `$NX_ROOT\samples\pdmconf`. Eseguire il comando riportato di seguito:
`pdm_perl pdm_edit.pl`

Viene visualizzato un menu.

6. Selezionare Z per modificare i server Tomcat Visualizer. Immettere A per aggiungere un nuovo server Tomcat Visualizer.

Viene richiesto di immettere un nome host.

7. Specificare il nome host secondario.

Viene salvato il nome host secondario e viene visualizzato un elenco di modelli.

8. Seguire le istruzioni fornite dall'utilità `pdm_edit.pl`.

La configurazione del server Tomcat Visualizer secondario viene completata.

Configurazione dei componenti Automazione supporto

CA Service Desk Manager installa e configura i componenti Automazione supporto seguenti:

- Client utente finale
- Interfaccia analista Automazione supporto
- Server

I componenti seguenti vengono installati e configurati separatamente:

- Agente utente finale
- IDE editor attività automatizzate

Importante È necessario installare l'opzione *supportautomation_url* dopo aver installato CA Service Desk Manager, oltre a configurare Automazione supporto durante la configurazione di CA Service Desk Manager. Per ulteriori informazioni sull'opzione *supportautomation_url*, vedere la *Guida in linea*.

Modalità di configurazione delle modalità server di Automazione supporto

Durante l'installazione è possibile configurare le modalità server di Automazione supporto seguenti:

- **Server principale:** se si seleziona il tipo di configurazione Server principale, il campo Nome host o IP viene impostato automaticamente sul nome host locale. Per Server principale è necessario specificare tutti i parametri, ad eccezione della sezione Porta interna e del campo Associa a IP nella sezione Server socket, che sono facoltativi.

Importante Quando si imposta l'opzione *supportautomation_url*, questo URL deve specificare l'URL del server principale di Automazione supporto e non deve fare riferimento al server proxy o al server di bilanciamento del carico.

Nota: se si seleziona l'opzione Server principale e si intende anche configurare uno o più server proxy del socket, è *necessario* impostare la porta esterna e il nome host del server socket sull'host del proxy del socket e della porta esterna. Per più proxy del socket, si imposta il Server socket sull'host e sulla porta esterna del server del servizio di bilanciamento del carico.

- **Server proxy socket:** se è stato configurato un server secondario CA Service Desk Manager, è possibile selezionare il tipo di configurazione Server proxy socket. Vengono visualizzati i valori predefiniti per i campi. Per Server proxy socket è necessario specificare tutti i parametri, ad eccezione del campo facoltativo Associa a IP nella sezione Configurazione Socket.
- **Server messaggio di routing:** se è stato configurato un server secondario CA Service Desk Manager, è possibile selezionare il tipo di configurazione Server messaggio di routing. Vengono visualizzati i valori predefiniti per i campi. Per Server messaggio di routing è necessario specificare tutti i parametri, ad eccezione del campo facoltativo Associa a IP nella sezione Configurazione Socket.

Modalità di configurazione di Automazione supporto su un server secondario

È possibile configurare Automazione supporto su un server CA Service Desk Manager secondario.

Nota: quando si configura Support Automation su un server CA Service Desk Manager secondario, modificare il valore dell'opzione *supportautomation_url* se è attualmente configurata per puntare a un'istanza di Automazione supporto nel server primario.

Per configurare Automazione supporto su un server secondario

1. Selezionare Automazione supporto nella Configurazione guidata.
2. Immettere le informazioni appropriate per i tipi di configurazione in uso sul server secondario, ad esempio il nome host e la porta di un server socket.

Importante Dopo aver definito il server Automazione supporto, non è possibile modificarne il ruolo come server primario o secondario.

3. Continuare seguendo le istruzioni sullo schermo per completare l'installazione.

Automazione supporto viene installato e configurato su un server CA Service Desk Manager secondario.

4. Aprire un prompt dei comandi e passare alla cartella \$NX_ROOT\samples\pdmconf.

5. Eseguire il comando riportato di seguito:

```
pdm_perl pdm_edit.pl
```

Viene visualizzato un menu.

6. Immettere M per modificare i server Tomcat di Automazione supporto. Immettere A per aggiungere un server Tomcat di Automazione supporto.

Viene richiesto di immettere un nome host e un tipo di server.

7. Specificare il nome host e il tipo di server secondario.

Viene salvato il nome host secondario e viene visualizzato un elenco di modelli.

8. Seguire le istruzioni fornite dall'utilità pdm_edit.pl.

La configurazione del server Tomcat secondario di Automazione supporto viene completata.

Modalità di configurazione delle attività automatiche

È possibile installare e configurare l'editor delle attività automatiche per gestire le attività automatiche usate dagli analisti Automazione supporto per fornire supporto agli utenti finali. L'utente può avviare un'attività automatica da un documento della conoscenza e dall'interfaccia self-service oppure l'analista può eseguire un'attività automatica durante una sessione di assistenza. Le attività automatiche offrono agli analisti informazioni dettagliate sul computer dell'utente finale. È possibile creare attività automatiche self-service che interagiscano con l'utente finale ed elaborino il suo input. Queste attività possono modificare il file system, il registro, scaricare software da installare e così via. Per configurare le attività automatiche, effettuare le seguenti operazioni:

1. Installare l'editor delle attività automatiche.

Avviare il programma di installazione dalla seguente ubicazione sul supporto di installazione:

`casd.nt\SAScriptWriter`

Nota: è possibile anche copiare il programma di installazione e distribuirlo agli utenti appropriati nel proprio ambiente di supporto.

L'editor delle attività automatiche viene installato.

2. Aprire l'editor delle attività automatiche.

Il programma di installazione dell'editor delle attività automatiche crea un collegamento sul desktop.

3. Impostare i seguenti parametri di connessione:

- a. Fare clic su Strumenti, Server.

Viene visualizzata la finestra di dialogo Configurazione server.

- b. Immettere il nome host e la porta.

Porta predefinita: 8070

- c. Immettere il nome utente e la password di un utente con accesso in lettura/scrittura all'editor delle attività automatiche, come l'analista Automazione supporto.

- d. Fare clic su Test.

- e. Fare clic su OK.

4. Creare le attività automatiche e caricarle sul server.

È possibile caricare attività pubbliche oppure assegnarle a titolari o sottotitolari specifici.

Importante Solo i ruoli del titolare Fornitore del servizio con il flag **Aggiorna oggetti pubblici abilitato** possono caricare le attività e le librerie sul server. Tutto il contenuto della libreria delle attività e il contenuto statico vengono memorizzati come dati pubblici.

L'installazione di Screen Painter Web

Nota: prima di installare questo componente, verificare e leggere le informazioni su come pianificare un'installazione corretta.

Screen Painter Web consente di personalizzare lo schema e l'interfaccia Web di CA Service Desk Manager. Per impostazione predefinita, viene installato nel server primario ma è anche possibile installarlo in un altro computer.

Installazione di Screen Painter Web

Se si intende utilizzare Screen Painter Web per gestire le personalizzazioni dello schema e dell'interfaccia Web in CA Service Desk Manager, avviare ed eseguire l'installazione in un server primario o secondario di CA Service Desk Manager.

Per installare Screen Painter Web

1. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su Screen Painter Web.
5. Selezionare la lingua e fare clic su OK.
6. Continuare seguendo le istruzioni sullo schermo per completare l'installazione di Screen Painter Web.

Screen Painter Web viene installato ed è possibile personalizzare lo schema e l'interfaccia Web.

Installazione dell'integrazione di CA NSM

Nota: prima di installare questo componente, verificare e leggere le informazioni su come pianificare un'installazione corretta.

È possibile installare l'integrazione di CA NSM nelle posizioni seguenti:

- Server CA Service Desk Manager primario
- Server CA Service Desk Manager secondario
- Server autonomo (non CA Service Desk Manager)

I componenti di integrazione di CA NSM vengono installati automaticamente nei server primario e secondario durante l'installazione del server CA Service Desk Manager. Su un server autonomo eseguire il componente dell'integrazione di CA NSM dal menu di installazione di CA Service Desk Manager.

Nota: questo componente viene eseguito solo su un server Windows che non sia un server CA Service Desk Manager primario o secondario. L'installazione dell'integrazione di CA NSM per un server primario o secondario viene eseguita automaticamente.

Ulteriori informazioni:

[Pianificazione dell'installazione di CA NSM](#) (a pagina 110)

[Installazione dell'integrazione di CA NSM \(Windows\)](#) (a pagina 137)

Installazione dell'integrazione di CA NSM (Windows)

Se si desidera integrare CA NSM e CA Service Desk Manager per il controllo automatico di eventuali problemi di gestione di rete e per coordinare automaticamente eventi di gestione critici, avviare ed eseguire l'installazione di integrazione di CA NSM su un server CA NSM su cui non sono presenti altri componenti di CA Service Desk Manager.

Per installare l'integrazione di CA NSM

1. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su Integrazione di CA NSM.
5. Seguire le istruzioni visualizzate e, quando richiesto, specificare le informazioni seguenti:
 - Nome host slump
 - Indirizzo IP host slump
 - ID porta slump
 - Repository NSM

Con il programma di installazione vengono creati il file NX.env e un servizio Windows per avviare e interrompere il Convertitore eventi.

6. Aggiornare il file topology.cfg nel server CA Service Desk Manager primario o secondario in modo che rifletta l'indirizzo IP remoto del server CA NSM.

È stata installata l'integrazione di CA NSM ed è possibile integrare i due prodotti.

Ulteriori informazioni:

[Modalità di integrazione con CA NSM](#) (a pagina 527)

Installazione di CA EEM

Nota: prima di installare questo componente, verificare e leggere le informazioni su come pianificare un'installazione corretta.

CA EEM autentica ed autorizza gli utenti di prodotti CA quali CA Workflow e Gestione dei servizi CA. Per autenticazione si intende la verifica della validità dell'utente del prodotto mediante ID utente e password o altre informazioni. Per autorizzazione si intende invece la conferma che l'utente connesso può utilizzare una determinata funzionalità nel prodotto.

Ogni volta che un utente prova ad accedere, CA EEM deve autenticare le informazioni e, una volta autenticato, concede o nega l'accesso. Ad esempio, per accedere all'Elenco lavori o all'IDE CA Workflow, un utente deve disporre di un record utente CA EEM. Se si utilizza CA Workflow in CA Service Desk Manager per gestire i propri processi aziendali, è necessario prima avviare ed eseguire l'installazione di CA EEM in un ambiente operativo supportato. Quindi, installare immediatamente CA Workflow.

Importante Nel caso di un'installazione di CA EEM esistente che è possibile utilizzare per autenticare i prodotti CA, non installare nuovamente CA EEM. Installare invece i prodotti CA e fare riferimento all'installazione di CA EEM esistente. Per l'integrazione CA Service Desk Manager r12.5 è tuttavia necessario disporre almeno di CA EEM r8.3.

Ulteriori informazioni:

[Pianificazione dell'installazione di CA EEM e CA Workflow](#) (a pagina 92)

[Installazione di CA EEM \(Windows\)](#) (a pagina 139)

[Installazione di CA EEM \(UNIX\)](#) (a pagina 140)

Installazione di CA EEM (Windows)

È possibile avviare ed eseguire l'installazione di CA EEM in un ambiente operativo supportato.

Importante Nel caso di un'installazione di CA EEM esistente che è possibile utilizzare per autenticare i prodotti CA, non installare nuovamente CA EEM. Installare invece i prodotti CA e fare riferimento all'installazione di CA EEM esistente. Per l'integrazione CA Service Desk Manager r12.5 è tuttavia necessario disporre almeno di CA EEM r8.3.

Per installare CA EEM

1. (Facoltativo) Verificare di avere installato JRE (Java Runtime Environment) 1.5 e di avere impostato la variabile JAVA_HOME.

Nota: è possibile ignorare questo passaggio in CA EEM 8.4 o versione successiva ma verrà visualizzato un avviso che segnala che non è possibile integrare CA SiteMinder e SAML.

2. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

3. Fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

4. Fare clic sulla scheda Installazione prodotto.
5. CA Embedded Entitlements Manager
6. Continuare seguendo le istruzioni visualizzate per completare l'installazione di CA EEM.

L'installazione di CA EEM viene completata ed è possibile installare altri prodotti CA.

Ulteriori informazioni:

[Pianificazione dell'installazione di CA EEM e CA Workflow](#) (a pagina 92)

Installazione di CA EEM (UNIX)

CA EEM per Linux e UNIX utilizza uno script con shell ad estrazione automatica che assiste l'utente durante il processo di installazione. Durante il processo di installazione, viene visualizzato un file di licenza e vengono richiesti i parametri di installazione. Dopo l'immissione dei parametri di installazione, inizia l'installazione.

Importante Nel caso di un'installazione di CA EEM esistente che è possibile utilizzare per autenticare i prodotti CA, non installare nuovamente CA EEM. Installare invece i prodotti CA e fare riferimento all'installazione di CA EEM esistente. Per l'integrazione CA Service Desk Manager r12.5 è tuttavia necessario disporre almeno di CA EEM r8.3.

Per installare CA EEM

1. Eseguire lo script appropriato sul computer di destinazione.
 - (Linux) /lnxsrvr.cd1/ca_tps.lnx/EEM/EEMServer.sh
 - (AIX) /aixsrvr.cd1/ca_tps.aix/EEM/EEMServer.sh
 - (Sun) /solsrvr.cd1/ca_tps.sol/EEM/EEMServer.shIl file viene decompresso e inizia l'installazione.
2. Immettere y per accettare i termini e le condizioni del contratto di licenza (oppure n per rifiutare e interrompere l'installazione).

Vengono richiesti i parametri di installazione.

3. Immettere i parametri di installazione.

Esempio:

- a. Immettere il percorso di installazione per CA EEM (oppure accettare quello predefinito).
- b. Se si intende installare CA EEM r8.4 o versione successiva, utilizzare il comando seguente per evitare di impostare la variabile JAVA_HOME:

```
/EEMServer.sh -javahome none
```

Nota: se si utilizza una versione precedente di CA EEM, immettere il valore da assegnare alla variabile \$JAVA_HOME quando richiesto. Nel programma di installazione iGateway la variabile JAVA_HOME viene utilizzata per individuare la JVM (Java Virtual Machine) necessaria per il corretto funzionamento del server CA EEM. Lo script del programma di installazione richiede tale variabile solo nel caso in cui non sia già stata impostata nell'ambiente.

Viene visualizzata una schermata di conferma contenente i valori dei parametri di installazione immessi.

4. Se le informazioni sulla schermata di conferma sono corrette, immettere Y per continuare l'installazione. Se si immette N, si interrompe l'esecuzione del programma di installazione.
5. Immettere la password EiamAdmin.

Nota: il nome utente predefinito dell'amministratore è EiamAdmin.

La procedura di installazione varia in base ai parametri della riga di comando e al tipo di pacchetto del server CA EEM che si sta installando.

L'installazione di CA EEM nel computer in uso viene completata mediante lo script del programma di installazione.

Parametri dello script di installazione CA EEM

Il programma di installazione per CA EEM accetta i parametri della riga di comando seguenti:

eiampath

Specifica il percorso in cui si desidera installare CA EEM. Il percorso predefinito è C:\Programmi\CA\SC\Embedded IAM.

etdirpath [percorso]

Specifica il percorso in cui si desidera installare CA Directory. Il percorso predefinito è C:\Programmi\CA\eTrust Directory.

igpath [percorso]

Specifica il percorso in cui si desidera installare iGateway. Il percorso predefinito è C:\Programmi\CA\SC\iTechnology.

ingpath [directory]

Specifica il percorso in cui si desidera installare Ingres. Il percorso predefinito è C:\Programmi\CA\Ingres [EI].

db [schema database]

Specifica l'utilizzo da parte di CA EEM dello schema del database iTechPoz con il server MDB CA EEM per la memorizzazione delle informazioni sulle norme.

Esempio

```
EEMServer_8.3_[builddate]_win32.exe -s -a /z"db=iTechpoz; "
```

Installazione di CA Workflow

Nota: prima di installare questo componente, verificare e leggere le informazioni su come pianificare un'installazione corretta.

Ogni volta che un utente prova ad accedere a CA Workflow, CA EEM autentica le informazioni e, una volta autenticate, concede o nega l'accesso. Nota: per accedere all'Elenco lavori o all'IDE CA Workflow, un utente deve disporre di un record utente CA EEM.

Dopo avere installato CA EEM, avviare ed eseguire l'installazione di CA Workflow in un server CA Service Desk Manager primario o secondario per gestire i processi aziendali.

Importante se si installa CA Workflow e si disinstalla CA Service Desk Manager, anche CA Workflow verrà disinstallato.

I registri CA Workflow (*pdm_install_wf.log* e *pdm_tomcat_CAWF.log*) si trovano in \$NX_ROOT/log. Se l'installazione di CA Workflow viene eseguita correttamente, \$NX_ROOT/site/Workflow/log include *wf_admin.log*, *wf_process.log*, *wf_security.log* e *wl_debug.log*.

Ulteriori informazioni:

[Pianificazione dell'installazione di CA EEM e CA Workflow](#) (a pagina 92)

[Installazione di CA Workflow \(Windows\)](#) (a pagina 143)

[Installazione di CA Workflow \(UNIX\)](#) (a pagina 144)

[Avvio e arresto di CA Workflow](#) (a pagina 211)

Installazione di CA Workflow (Windows)

Se si desidera utilizzare CA Workflow per gestire i processi aziendali in CA Service Desk Manager, avviare ed eseguire l'installazione di CA Workflow in un server CA Service Desk Manager primario o secondario.

Per installare CA Workflow

1. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su CA Workflow.
5. Continuare seguendo le istruzioni sullo schermo per completare l'installazione di CA Workflow.

CA Workflow viene installato ed è possibile configurarlo per l'uso con CA Service Desk Manager.

Ulteriori informazioni:

[Modalità di configurazione del flusso di lavoro di esempio per Gestione dei problemi](#) (a pagina 219)

[Integrazione di CA Workflow](#) (a pagina 521)

Installazione di CA Workflow (UNIX)

Se si desidera utilizzare CA Workflow per gestire i processi aziendali in CA Service Desk Manager, avviare ed eseguire l'installazione di CA Workflow in un server CA Service Desk Manager primario o secondario.

Per installare CA Workflow

1. Inserire il supporto di installazione sulla propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Accedere alla directory principale del supporto di installazione e avviare l'installazione eseguendo il comando seguente:

```
sh ./setup.sh
```

3. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

4. Fare clic sulla scheda Installazione prodotto.

5. Fare clic su CA Workflow.

6. Continuare seguendo le istruzioni visualizzate per completare l'installazione di CA Workflow.

L'installazione di CA Workflow viene completata ed è possibile eseguire la configurazione per l'uso con CA Service Desk Manager.

Ulteriori informazioni:

[Modalità di configurazione del flusso di lavoro di esempio per Gestione dei problemi](#) (a pagina 219)

[Integrazione di CA Workflow](#) (a pagina 521)

Installazione di CA Workflow IDE standalone

È possibile installare il client standalone CA Workflow IDE dal supporto di installazione di CA Service Desk Manager in Windows e Linux. Per le installazioni UNIX, questo client consente la connessione al server CA Workflow UNIX. È possibile puntare a qualsiasi installazione del server CA Workflow indipendentemente dall'ambiente operativo cambiando l'URL nella rispettiva GUI di accesso.

Per l'installazione di CA Workflow IDE non è necessario CA Service Desk Manager. Il percorso del registro di installazione è diverso nei sistemi con o senza CA Service Desk Manager.

- Se CA Service Desk Manager è installato in Windows e Linux, il registro si trova nel percorso seguente:
\$NX_ROOT/logs
- Se CA Service Desk Manager non è installato, il registro si trova nelle cartelle temporanee seguenti:

Windows

%temp%

Linux

/tmp

Per installare CA Workflow IDE in Windows o Linux

1. Aprire il supporto di installazione e selezionare CA Workflow IDE.
Viene visualizzata la procedura guidata di installazione dei componenti di CA Service Desk Manager.
2. Specificare il Percorso di installazione client del flusso di lavoro
3. Fare clic su Avanti.
L'installazione viene così completata.

Verifica dell'installazione di CA Workflow IDE

È *necessario* verificare che l'installazione di CA Workflow IDE sia stata completata correttamente.

Per verificare l'installazione di CA Workflow IDE

1. Passare alla directory specificata nel campo Percorso di installazione client flusso di lavoro nella procedura guidata di installazione dei componenti CA Service Desk Manager.
2. Verificare che la directory contenga gli elementi seguenti:
 - Cartelle denominate "Client" e "uninstall"
 - File denominati *version.txt* e *wekinstall.log*

Nota: se l'installazione presenta errori oppure se le cartelle e i file si trovano nel percorso sbagliato, visualizzare il file *pdm_install_wf_client.log*.

In Windows è possibile avviare CA Workflow IDE dal menu Start selezionando Programmi, CA, Service Desk, CA Workflow IDE.

Disinstallare il client CA Workflow IDE (Windows e Linux)

Per disinstallare il client CA Workflow IDE

1. Eseguire il comando riportato di seguito:

```
<percorso_installazione>\jre\bin\java" -cp "<percorso_installazione>\uninstall\uninstall.jar" run -silent
```

percorso_installazione

Specifica la cartella principale in cui è stato installato il client CA Workflow IDE.

■ **Esempio per Windows**

Se "c:\test" è la cartella principale in cui è stato installato il client CA Workflow IDE:

```
"c:\test\jre\bin\java" -cp "c:\test\uninstall\uninstall.jar" run -silent
```

■ **Esempio per Linux**

Se "/test" è la cartella principale in cui è stato installato il client CA Workflow IDE:

```
"/test/jre/bin/java" -cp "/test/uninstall/uninstall.jar" run -silent
```

2. Eliminare la cartella principale in cui è stato installato il client CA Workflow IDE.
3. (Windows) Eliminare il collegamento associato del menu di avvio.

Installazione di ADT

Prima di installare il componente ADT, verificare e leggere le istruzioni per pianificare un'installazione riuscita.

Ulteriori informazioni:

[Installazione di ADT](#) (a pagina 147)

Installazione di ADT

È possibile configurare ADT per l'ambiente in uso.

Nota: ADT non è certificato su Windows 2000.

Per installare ADT

1. Accedere come amministratore al computer in cui si desidera installare ADT e inserire il supporto di installazione nell'unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su Advantage Data Transformer.
5. Per continuare con l'installazione, seguire le istruzioni sullo schermo.

Viene visualizzata la Configurazione guidata.

6. Immettere e selezionare le informazioni per configurare il prodotto.
7. Continuare seguendo le istruzioni sullo schermo per completare l'installazione.

ADT è ora installato.

8. Fare clic su Sì per riavviare il computer e procedere con l'installazione dei Federation Adapters.

Patch ADT: caratteri non UTF-8

Sintomo:

Per impostazione predefinita, ADT utilizza il set di caratteri UTF-8 (Unicode) per la generazione del documento di input XML che viene letto da GRLoader. Questo comporta pertanto la creazione di un documento XML non valido.

Il documento non è valido in quanto specifica la presenza di caratteri UTF-8, ma è possibile che contenga altri caratteri. Quando si tenta di eseguire la lettura di questo documento non valido in GRLoader, verrà generata un'eccezione UTFDataFormatException nel file di registro GRLoader.log e non sarà possibile importare i dati in CMDB.

Soluzione:

Può essere opportuno utilizzare un set di caratteri alternativo al set di caratteri UTF-8. Per utilizzare un set di caratteri non UTF-8, effettuare le operazioni seguenti:

1. Eseguire una ricerca su ISO-8859 per individuare un set di caratteri più adatto.
2. Individuare un set di caratteri alternativo.

La soluzione pubblicata ADT QO87072 (disponibile nel sito support.ca.com) consente di modificare il set di caratteri predefinito da UTF-8 in un altro set di caratteri.

3. Installare la correzione e modificare il Registro di sistema Windows in base alle istruzioni.

GRLoader è in grado di caricare i dati, inclusi i caratteri non UTF-8 necessari.

L'installazione di Federation Adapters di CA CMDB

Nota: prima di installare questo componente, verificare e leggere le informazioni su come pianificare un'installazione corretta.

I Federation Adapters di CA CMDB consentono di importare dati di terze parti in CA CMDB. Prima di installare i Federation Adapters di CA CMDB nell'ambiente operativo (SQL Server o Oracle), creare un ID utente ADT e configurarlo nel database.

Ulteriori informazioni:

[Creazione dell'ID amministratore \(SQL Server\)](#) (a pagina 149)

[Configurazione di ADT \(SQL Server\)](#) (a pagina 150)

[Creazione dell'ID amministratore e configurazione di ADT \(Oracle\)](#) (a pagina 151)

[Installazione dei Federation Adapters di CA CMDB](#) (a pagina 152)

Creazione dell'ID amministratore (SQL Server)

Quando si utilizza un database SQL Server, l'ID dell'amministratore del database deve disporre di privilegi sufficienti a creare un utente. In SQL Server è necessario assegnare all'utente il ruolo **sysadmin** o **securityadmin**. L'ID dell'amministratore e dell'utente CMDBAdmin specificati durante un'installazione remota di MDB non hanno privilegi sufficienti per creare l'ID utente ADT (infopump). L'amministratore del sistema predefinito **sa** è in grado di creare ID di accesso SQL Server.

Per creare l'ID amministratore e configurare ADT

1. Accedere come amministratore al computer in cui si desidera installare i Federation Adapters di CA CMDB e inserire il supporto di installazione nell'unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic sul collegamento Installare Federation Adapters di CA CMDB.
5. Per continuare con l'installazione, seguire le istruzioni sullo schermo.

Viene visualizzata la pagina iniziale.

Viene visualizzata la Configurazione guidata.

Nota: il campo dell'ID amministratore per ADT viene compilato automaticamente e non può essere modificato.

Un messaggio informa che l'ID ADT infopump è stato creato.

6. Immettere IDB nel campo Nome. Nel campo Server, selezionare il server di database dall'elenco a discesa.

Nota: se il server di database desiderato non è disponibile nell'elenco a discesa, è possibile immettere manualmente un *nome host* oppure un *nome host\nome istanza* (per un'istanza con nome SQL Server) nel campo Server.

7. Continuare seguendo le istruzioni sullo schermo per completare l'installazione.

8. Fare clic su Fine.

Viene visualizzata una pagina di verifica.

9. Fare clic su Verifica fonte dati.

La fonte dati ODBC creata verrà sottoposta a verifica. Al completamento del test, viene visualizzato un messaggio che ne conferma l'esito positivo.

Configurazione di ADT (SQL Server)

È necessario configurare ADT per poter installare i Federation Adapters di CA CMDB. La configurazione di ADT inizia immediatamente dopo la creazione dell'ID amministratore da parte di ADT.

Per configurare ADT

1. Fare clic su OK nella schermata di esito positivo.

Viene creata l'origine dati ODBC SQL Server e visualizzata la pagina di accesso a ODBC.

2. Immettere l'ID utente e la password richiesti per accedere al database e fare clic su Avanti.

Viene visualizzata la pagina Server ADT.

3. Seguire le istruzioni visualizzate.

4. Fare clic su OK e su Chiudi nelle pagine e nei messaggi visualizzati.

Inizia la configurazione del gestore script e viene visualizzata la pagina Configurazione ADT.

5. Fare clic su Avanti per confermare il gestore script selezionato.

Viene visualizzata la pagina Riepilogo.

6. Fare clic su Fine.

È ora possibile installare i Federation Adapters.

Creazione dell'ID amministratore e configurazione di ADT (Oracle)

Quando si utilizza un database Oracle, creare un ID amministratore e configurare ADT.

Per creare l'ID amministratore e configurare ADT

1. Accedere come amministratore al computer in cui si desidera installare i Federation Adapters di CA CMDB e inserire il supporto di installazione nell'unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
 4. Fare clic sul collegamento Installare Federation Adapters di CA CMDB.
- Viene visualizzata a pagina Impossibile determinare il tipo di database.

5. Immettere Oracle come tipo di database e fare clic su OK.

Viene visualizzata la pagina Crea ADT.

6. Continuare seguendo le istruzioni sullo schermo per completare l'installazione.
7. Fare clic su Fine.

L'operazione viene completata correttamente.

Installazione dei Federation Adapters di CA CMDB

L'installazione del Federation Adapter di CA CMDB inizia al termine della configurazione di CA Advantage Data Transformer. In alternativa, è possibile installarlo dal supporto di installazione.

Per installare i Federation Adapters sul database

1. Accedere come amministratore al computer in cui si desidera installare CA Advantage Data Transformer e inserire il supporto di installazione nell'unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su CA Advantage Data Transformer nella pagina Installazione prodotto.
5. Immettere la password per l'ID di amministratore di CA Advantage Data Transformer (infopump).
6. Accertarsi che IDB sia selezionato come fonte dati ODBC e fare clic su OK.

La pagina di stato dell'installazione dei Federation Adapters visualizza il progresso e il completamento dell'installazione.

Installazione di FAST ESP

Prima di installare questo componente, verificare e leggere le informazioni su come pianificare un'installazione corretta.

Se si desidera integrare FAST ESP con la funzionalità Gestione delle informazioni di CA Service Desk Manager, installare il motore di ricerca FAST ESP. Avviare ed eseguire l'installazione del motore del modulo di ricerca FAST ESP in un server autonomo dedicato. Se si installa CA Service Desk Manager e FAST ESP nello stesso computer, avviare sempre CA Service Desk Manager prima di FAST ESP per evitare conflitti di porta.

Nota: per ulteriori informazioni, vedere le *Note di rilascio*.

Importante per dettagli completi sui prerequisiti di installazione, vedere *FAST ESP Installation Guide*, disponibile in `\CA_tps.nt\FastESP\Doc\en-US`. Nella documentazione di FAST ESP sono illustrati diversi scenari di installazione, tuttavia CA Service Desk Manager supporta l'integrazione con FAST ESP solo quando viene installato dal supporto di installazione di CA Service Desk Manager.

Ulteriori informazioni:

[Pianificazione dell'installazione di FAST ESP](#) (a pagina 111)

[Installazione di FAST ESP \(Windows\)](#) (a pagina 153)

[Installazione di FAST ESP \(Linux\)](#) (a pagina 154)

[Installazione di LinguisticsStudio](#) (a pagina 156)

Installazione di FAST ESP (Windows)

Se si desidera integrare FAST ESP con la funzionalità Gestione delle informazioni di CA Service Desk Manager per migliorare le proprie ricerche nella conoscenza, avviare ed eseguire l'installazione del motore di ricerca FAST ESP in un server autonomo dedicato.

Per installare il motore del modulo di ricerca FAST ESP

1. Inserire il supporto di installazione nella propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

Nota: se il menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe nella directory principale del supporto di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su FAST ESP.
5. Continuare seguendo le istruzioni visualizzate per completare l'installazione di FAST ESP.

L'installazione del motore di ricerca FAST ESP viene completata ed è possibile eseguire la configurazione per l'uso con CA Service Desk Manager in Gestione opzioni.

Nota: per ulteriori informazioni, consultare la *Guida all'amministrazione*.

Ulteriori informazioni:

[Il registro di installazione di FAST ESP](#) (a pagina 155)

[Modalità di configurazione di FAST ESP](#) (a pagina 195)

[Modalità di esecuzione del backup dei dati di FAST ESP](#) (a pagina 208)

Installazione di FAST ESP (Linux)

Se si desidera integrare FAST ESP con la funzionalità Gestione delle informazioni di CA Service Desk Manager per migliorare le proprie ricerche nella conoscenza, avviare ed eseguire l'installazione del motore di ricerca FAST ESP in un server autonomo dedicato.

Per installare il motore del modulo di ricerca FAST ESP

1. Inserire il supporto di installazione sulla propria unità.

Importante se il computer non dispone di un'unità appropriata per i supporti di installazione, copiare il contenuto dei supporti nel computer in cui si desidera installare CA Service Desk Manager. Quindi, avviare l'installazione. Per un'installazione remota in rete, è possibile condividere un'unità o una cartella di rete e quindi connettersi alla rete per avviare l'installazione.

2. Accedere alla directory principale del supporto di installazione e avviare l'installazione eseguendo il comando seguente:

```
sh ./setup.sh
```

3. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.
Viene visualizzato il menu di installazione.
4. Fare clic sulla scheda Installazione prodotto.

5. Fare clic su FAST ESP.
6. Continuare seguendo le istruzioni visualizzate per completare l'installazione di FAST ESP.

L'installazione del motore di ricerca FAST ESP viene completata ed è possibile eseguire la configurazione per l'uso con CA Service Desk Manager in Gestione opzioni.

Nota: per ulteriori informazioni, consultare la *Guida all'amministrazione*.

Ulteriori informazioni:

[Il registro di installazione di FAST ESP](#) (a pagina 155)

[Modalità di configurazione di FAST ESP](#) (a pagina 195)

[Modalità di esecuzione del backup dei dati di FAST ESP](#) (a pagina 208)

Il registro di installazione di FAST ESP

Quando si installa il motore del modulo di ricerca FAST ESP, viene creato un file di registro dell'installazione per documentare ed elencare le azioni, gli eventi e i cambiamenti di sistema verificatisi durante l'installazione. Se il prodotto non viene installato correttamente, è possibile visualizzare gli errori nel file di registro per risolvere eventuali problemi e consentire la corretta installazione del motore di ricerca.

Il file di registro dell'installazione di FAST ESP si trova nella cartella `\KTInstallLog` della directory di installazione di FAST ESP. Per impostazione predefinita, la directory principale per l'installazione di FAST ESP è `C:\FastESP` (Windows) e `/opt/FastESP` (Linux). Aprire il file con un editor di testo quale Blocco note o l'editor vi.

Importante Quando si installa FAST ESP in un server dove è stata abilitata l'opzione relativa all'ora legale, si verifica un problema noto. Per maggiori informazioni sulla risoluzione di questo problema, vedere le *Note di rilascio*.

Installazione di LinguisticsStudio

LinguisticsStudio (un componente di prodotto di FAST ESP) consente di configurare la lemmatizzazione per l'indicizzazione dei documenti e l'elaborazione delle query. È inoltre possibile utilizzare LinguisticsStudio per creare e modificare i dizionari dei sinonimi.

Installare LinguisticsStudio per configurare la funzionalità dei sinonimi con FAST ESP. Completare i passaggi seguenti nel computer FAST ESP in cui si desidera installare LinguisticsStudio.

Per installare LinguisticsStudio

1. Installare il JDK (Java development kit) 6 (jdk-6u7-windows-i586-p.exe).
2. Impostare la variabile di ambiente JAVA_HOME in modo che faccia riferimento a JDK 6. Ad esempio, JAVA_HOME=c:\jdk6.
3. Aggiungere la posizione di JDK 6 alla variabile di ambiente PATH. Ad esempio, c:\jdk6\bin.
4. Estrarre \$FASTROOT/LinguisticsStudio/linguisticsstudio-1.23-win32.win32.x86.zip in una cartella \$ls.
5. Scaricare i file seguenti necessari per l'installazione in base a \$ls/installer/lingstudio_install.xml:
 - eclipse-SDK-3.2.1-win32.zip
 - hibernate-3.0.5.zip
 - JacORB_2_2_1-compact.zip
 - xxl_1_0.zip
6. Dopo aver scaricato tutti i file precedenti, copiarli nella cartella www nella directory ESP in cui si desidera installare LinguisticsStudio. Seguono esempi di cartelle:
 - \$FASTROOT\www\xxl_1_0.zip
 - \$FASTROOT\www\JacORB_2_2_1-compact.zip
 - \$FASTROOT\www\hibernate-3.0.5.zip
 - \$FASTROOT\www\eclipse-SDK-3.2.1-win32.zip

7. Aggiornare il file *lingstudio_install.xml* in modo che rifletta il nuovo percorso URL dei file (se si sta eseguendo l'installazione nello stesso computer del nodo Admin). Di seguito vengono presentati esempi di voci URL di *lingstudio_install.xml*:
 - `<mirror>http://localhost:16000/xxl_1_0.zip</mirror>`
 - `<mirror>http://localhost:16000/JacORB_2_2_1-compact.zip</mirror>`
 - `<mirror>http://localhost:16000/hibernate-3.0.5.zip</mirror>`
 - `<mirror>http://localhost:16000/eclipse-SDK-3.2.1-win32.zip</mirror>`
8. Eseguire il comando `$ls/setup.cmd` per distribuire i file richiesti in base al file *lingstudio_install.xml* aggiornato.
9. Eseguire il comando `$ls/linguisticsstudio/linguisticsstudio.exe`.

Ulteriori informazioni:

[Il registro di installazione di FAST ESP](#) (a pagina 155)

[Configurazione dei sinonimi](#) (a pagina 203)

[Modalità di configurazione di FAST ESP](#) (a pagina 195)

[Modalità di esecuzione del backup dei dati di FAST ESP](#) (a pagina 208)

Installazione di CA Business Intelligence

Nota: prima di installare questo componente, verificare e leggere le informazioni su come pianificare un'installazione corretta.

Se si desidera utilizzare CA Business Intelligence con CA Service Desk Manager per personalizzare i report esistenti o progettare report personalizzati, installare CA Business Intelligence. Generalmente l'installazione di CA Business Intelligence viene avviata ed eseguita in un server autonomo dedicato.

Durante l'installazione, si crea una password per l'amministratore di BusinessObjects. Questa password *deve* essere composta da almeno sei caratteri, sia minuscoli che maiuscoli, e non può contenere la parola *amministratore* o eventuali varianti. È consigliabile che la password contenga almeno due dei tipi di caratteri seguenti:

- Maiuscolo
- Minuscolo

- Numerico
- Segno di punteggiatura

Importante Apache Tomcat viene selezionato automaticamente per un'installazione rapida. Se si seleziona Personalizzata, è *necessario* selezionare Apache Tomcat se si intende utilizzare la scheda Report di CA Service Desk Manager.

Nota: per ulteriori informazioni su CA Business Intelligence, consultare la *Guida all'installazione di CA Business Intelligence*.

Ulteriori informazioni:

[Pianificazione dell'installazione di CA Business Intelligence](#) (a pagina 105)
[Installazione nuova di CA Business Intelligence](#) (a pagina 158)

Installazione nuova di CA Business Intelligence

Se si desidera utilizzare CA Business Intelligence con CA Service Desk Manager per personalizzare i report esistenti o progettare report personalizzati, avviare ed eseguire l'installazione di CA Business Intelligence in un server autonomo dedicato.

Importante Non installare CA Business Intelligence nello stesso computer in cui è installato FAST ESP.

Per installare CA Business Intelligence

1. Inserire il supporto di installazione nella propria unità.

Importante Se il computer non dispone di un'unità appropriata per il supporto di installazione, copiare il contenuto del supporto nel computer in cui si desidera installare CA Business Intelligence. Quindi, avviare l'installazione. Per avviare un'installazione remota in rete, potrebbe inoltre essere necessario condividere un'unità o una cartella in rete, quindi connettersi in rete.

Viene visualizzato il menu di installazione.

Nota: se il Menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe, presente sulla directory principale del supporto di installazione.

2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.

Viene visualizzato il menu di installazione.

3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su Installazione di CA Business Intelligence.

Importante Il collegamento Configurazione CA Business Intelligence consente di eseguire alcuni passaggi successivi all'installazione e alla configurazione che è necessario completare solo dopo avere installato CA Business Intelligence.

5. Continuare seguendo le istruzioni visualizzate per completare l'installazione di CA Business Intelligence.

Nota: per ulteriori istruzioni di installazione, consultare la *Guida all'implementazione di CA Business Intelligence*.

L'installazione di CA Business Intelligence viene completata ed è possibile eseguire la configurazione per l'uso con CA Service Desk Manager.

Nota: se viene richiesto, riavviare il computer alla fine dell'installazione.

Ulteriori informazioni:

[Modalità di configurazione di CA Business Intelligence](#) (a pagina 173)
[Configurazione delle impostazioni iniziali di CA Business Intelligence](#) (a pagina 174)

Installazione personalizzata di CA Business Intelligence (Windows)

Se si utilizza un database diverso da MySQL, è *necessario* creare il database CMS prima di eseguire un'installazione personalizzata di CA Business Intelligence.

Se si sceglie il database Microsoft SQL, effettuare le operazioni seguenti:

1. Creare un database CMS.

Nota: BusinessObjects Enterprise richiede un database per archiviare le informazioni su utenti e gruppi, livelli di protezione, contenuto BusinessObjects Enterprise e server. Il database primario, gestito da CMS, è noto come database CMS. Nel corso dell'installazione di CA Business Intelligence, si indica il CMS da utilizzare e si immettono i parametri necessari per l'autenticazione. Per ulteriori informazioni sui requisiti e sulla preparazione del database CMS, consultare la *Guida all'implementazione di CA Business Intelligence*.

2. Se si desidera utilizzare un database separato per il controllo, creare un database di controllo CMS.
3. Creare un account utente per il database CMS con *db_accessadmin*, *db_owner* e *db_securityadmin* come membri del ruolo e schemi di proprietà.

4. Se è stato creato un database di controllo CMS separato, creare un account utente per tale database con *db_accessadmin*, *db_owner* e *db_securityadmin* come membri del ruolo e schemi di proprietà.
5. Creare un DSN per il database CMS e il database di controllo CMS (se utilizzato). ato
6. Eseguire un'installazione personalizzata e, quando viene richiesto di selezionare un tipo di database, selezionare l'opzione relativa all'utilizzo del DBMS esistente e di Microsoft SQL Server.

Nota: è necessaria una connessione ODBC a 32 bit per CA Business Intelligence 3.0. In un sistema a 64 bit, è possibile creare facilmente una connessione ODBC a 32 bit eseguendo la versione a 32 bit di "create dsn". Per creare questa connessione, richiamare odbcad32.exe dalla directory C:\Windows\SysWow64.

Se si sceglie il database Oracle, effettuare le operazioni seguenti:

1. Installare il server di database Oracle e configurare il server per l'utilizzo della codifica Unicode per i tipi carattere.
2. Verificare che le variabili di ambiente Oracle siano impostate correttamente.
3. Creare un database e un utente per il database CMS.

Nota: quando si creano i database CMS e CMS di controllo, è *necessario* utilizzare il nome *tns*, il nome utente e la password specificati durante l'installazione di Business Objects.

4. Creare un database e un utente per il database di controllo CMS (se si desidera utilizzare un database separato per il controllo).
5. Eseguire un'installazione personalizzata e, quando viene richiesto di selezionare un tipo di database, selezionare l'opzione relativa all'utilizzo del DBMS esistente e di Oracle.

Esecuzione di un'installazione personalizzata

Un'installazione personalizzata consente di selezionare e configurare le funzionalità da installare.

Per eseguire un'installazione personalizzata di CA Business Intelligence

1. Immettere e confermare la password di amministratore di BusinessObjects XI.
2. Selezionare il tipo di database CMS.

Per amministrare il database CMS, impostare un account di database per CA Business Intelligence come indicato di seguito:

Microsoft SQL o Oracle:

- Creare o selezionare un account utente che fornisce a BusinessObjects Enterprise i privilegi necessari per accedere al proprio server di database.
- Verificare che si è in grado di effettuare l'accesso al database e svolgere operazioni amministrative con l'account impostato per il CMS.

Per MySQL

- Se si desidera installare MySQL quando si installa CA Business Intelligence, viene richiesto di impostare questo account durante l'installazione.

3. Specificare le proprietà di connessione del database.

Microsoft SQL Server:

Configurare il database prima dell'installazione. Creare quindi una fonte dati utilizzando Amministratore fonte dati ODBC nella scheda DSN di sistema per la connessione.

- Fare clic su Microsoft SQL Server e quindi su Avanti.
- Immettere il nome DNS.
- Immettere il nome del database.
- Immettere il nome utente.
- Immettere e confermare la password.

Ripetere questi passaggi per il database di controllo se si prevede di utilizzarne uno, quindi fare clic su Avanti. In caso contrario, fare clic su Avanti. Se si seleziona "Utilizza le stesse impostazioni per il database di controllo", le impostazioni di connessione del database CMS verranno applicate al database di controllo.

Per Oracle:

- Fare clic su Oracle.
- Immettere il nome *tns* Oracle nel campo Nome TNS.
- Immettere le credenziali per il server nei campi Nome utente e Password.
- Ripetere questi passaggi per il database di controllo se si prevede di utilizzarne uno, quindi fare clic su Avanti. In caso contrario, fare clic su Avanti. Se si seleziona "Utilizza le stesse impostazioni per il database di controllo", le impostazioni di connessione del database CMS verranno applicate al database di controllo.

Per MySQL

- Fare clic su MySQL.
- Immettere il nome del database per il database CMS nel campo Database.
- Immettere il nome host nel campo Nome host MySQL.
- Immettere la porta utilizzata da MySQL nel campo Porta.
- Immettere le credenziali per il server nei campi Nome utente e Password.
- Ripetere questi passaggi per il database di controllo se si prevede di utilizzarne uno, quindi fare clic su Avanti. In caso contrario, fare clic su Avanti. Se si seleziona "Utilizza le stesse impostazioni per il database di controllo", le impostazioni di connessione del database CMS verranno applicate al database di controllo.

4. Specificare la configurazione del server Web. CA Business Intelligence offre la possibilità di installare la propria versione di Apache Tomcat oppure di utilizzare il server applicazioni esistente.

Per Apache Tomcat

- Fare clic su Tomcat.
- Immettere la posizione dell'installazione di Apache Tomcat esistente.

Nota: quando Tomcat è già installato, il programma di installazione richiede solo questa informazione.

- Immettere il numero di porta di connessione Tomcat.

Nota: è consigliabile cambiare il numero di porta di *connessione* predefinito per evitare che l'utilizzo di questo numero di porta comune comporti interferenze con altre applicazioni. La porta di connessione consigliata per un'installazione tipica è 8070.

- Immettere il numero di porta di reindirizzamento Tomcat.
- Immettere il numero di porta di arresto Tomcat.

Nota: è consigliabile cambiare il numero di porta di *arresto* predefinito per evitare che l'utilizzo di questo numero di porta comune comporti interferenze con altre applicazioni. La porta di arresto consigliata per un'installazione tipica è 8075.

5. Specificare se installare database e modelli di esempio.
6. Controllare le impostazioni e installare CA Business Intelligence.

Procedere con il capitolo della *Guida all'implementazione di CA Business Intelligence* relativo al tipo di installazione selezionato.

Verifica dell'installazione

Dopo avere installato CA Service Desk Manager, utilizzare le informazioni seguenti per verificare la correttezza dell'installazione.

1. Verificare che per il prodotto sia stata impostata una variabile di ambiente di sistema per il percorso nella directory di installazione specificata. La directory principale predefinita è C:\Programmi\CA\Service Desk Manager.
2. Verificare che:
 - a. Nel Pannello di controllo (Installazione applicazioni) sia visualizzata una voce per il prodotto.
 - b. Dal menu Start che sia visualizzata un'opzione per:
 - Visualizzare la documentazione.
 - Avviare la Configurazione guidata.
 - Avviare l'interfaccia Web.
 - Contattare il supporto tecnico.
 - Avviare Screen Painter Web.
 - Disinstallare CA Service Desk Manager.
3. Verificare che sia possibile avviare l'interfaccia Web.

Importante se non è possibile verificare queste informazioni, il prodotto non è stato installato correttamente. In questo caso, avviare nuovamente l'installazione di CA Service Desk Manager per modificarla.

Ulteriori informazioni:

[Avvio dell'interfaccia Web](#) (a pagina 172)

Il registro di installazione

Quando si installa CA Service Desk Manager, viene creato un file di registro dell'installazione per documentare ed elencare le azioni, gli eventi e i cambiamenti di sistema verificatisi durante l'installazione. Se il prodotto non viene installato correttamente, è possibile visualizzare gli errori nel file di registro per risolvere eventuali problemi e consentire la corretta installazione del prodotto.

È possibile individuare il file *ServiceDesk_r12_5_Install.log* nella cartella \log della directory di installazione. Per l'installazione dei componenti remoti, il file di registro si trova nella directory %TEMP%. Aprire il file con un editor di testo quale Blocco note o l'editor vi.

Nota: se si annulla l'installazione prima che sia completa, il file di registro dell'installazione viene creato sul desktop (Windows) o nella directory principale (UNIX e Linux).

Capitolo 5: Configurazione

Questa sezione contiene i seguenti argomenti:

- [Configurazione del prodotto](#) (a pagina 165)
- [Configurazione dei componenti CA Service Desk Manager](#) (a pagina 166)
- [Modalità di configurazione dell'interfaccia Web](#) (a pagina 169)
- [Modalità di configurazione di CA Business Intelligence](#) (a pagina 173)
- [Esecuzione delle Norme automatiche](#) (a pagina 193)
- [Esecuzione della scheda Report della conoscenza](#) (a pagina 194)
- [Importazione di dati di esempio di Gestione delle informazioni](#) (a pagina 194)
- [Modalità di configurazione di FAST ESP](#) (a pagina 195)
- [Modalità di configurazione di CA Workflow](#) (a pagina 210)
- [Modalità di configurazione dell'integrazione del flusso di lavoro di CA IT PAM](#) (a pagina 226)
- [Impostazione dell'accesso automatico \(autenticazione CA MDB\)](#) (a pagina 233)
- [Configurazione di punti di ingresso singoli](#) (a pagina 235)
- [Modalità di implementazione della funzione multi-tenancy](#) (a pagina 236)

Configurazione del prodotto

Dopo avere installato CA Service Desk Manager ed eventuali prodotti aggiuntivi selezionati, è necessario completare alcune procedure di configurazione per consentire il corretto funzionamento dei prodotti. Per configurare il prodotto, completare la procedura seguente:

- Configurare i componenti di CA Service Desk Manager (server primario e secondario, il database, l'interfaccia Web).
- Configurare l'interfaccia Web quando il server Web e il server primario si trovano in computer diversi.
- Configurare Automazione supporto.
- Implementare report relativi al ciclo di vita di documenti della conoscenza per le Norme automatiche.
- Configurare CA Business Intelligence.
- Configurare CA Workflow.
- Configurare FAST ESP.
- Implementare il supporto multi-tenancy.

Ulteriori informazioni:

[Configurazione dei componenti CA Service Desk Manager](#) (a pagina 166)

[Modalità di configurazione dell'interfaccia Web](#) (a pagina 169)

[Esecuzione delle Norme automatiche](#) (a pagina 193)

[Modalità di configurazione di CA Business Intelligence](#) (a pagina 173)

[Modalità di configurazione del flusso di lavoro di esempio per Gestione dei problemi](#) (a pagina 219)

[Modalità di configurazione di FAST ESP](#) (a pagina 195)

[Modalità di implementazione della funzione multi-tenancy](#) (a pagina 236)

Configurazione dei componenti CA Service Desk Manager

Se non si configura CA Service Desk Manager durante l'installazione, oppure se si configura manualmente il prodotto dopo l'installazione, è possibile utilizzare il prodotto per configurare i server primario e secondario, il database, l'interfaccia Web e opzioni di configurazione aggiuntive.

Per verificare che sia possibile configurare correttamente il prodotto e i componenti in SQL Server, abilitare TCP/IP nel computer in cui si desidera eseguire l'installazione e la configurazione.

Nota: se gli host protocollo Internet versione 4 (IPv4) e protocollo Internet versione 6 (IPv6) coesistono sulla rete, verificare che siano utilizzate le strategie, gli strumenti e i meccanismi di transizione appropriati per supportare tali tecnologie prima di avviare la configurazione del prodotto. Per informazioni sulla configurazione dei server, vedere la *Guida all'amministrazione*.

Per configurare i componenti del prodotto

1. Selezionare Start, Programmi, CA, Service Desk, Configurazione.

Viene visualizzata la Configurazione guidata.

2. Immettere e selezionare le informazioni per configurare il prodotto.

Nota: per informazioni sui campi della procedura guidata, vedere la *Guida in linea alla configurazione del server*.

3. Continuare seguendo le istruzioni visualizzate per completare la configurazione del prodotto.

La prima volta che si esegue la configurazione, viene visualizzato un numero di servizio TCP predefinito che è valido per la maggior parte delle installazioni. Per determinare il numero di servizio TCP per la propria installazione, aprire una sessione telnet tra la workstation Windows e il server:

- Se la rete utilizza NIS, immettere:

```
ypcat services | grep slump.
```

L'output include una riga simile alla seguente:

```
slump nnnn/tcp #Richiesto per l'esecuzione slump.
```

- Se la rete non utilizza NIS, immettere:

```
grep slump /etc/services.
```

L'output include una riga simile alla seguente:

```
#slump nnnn/tcp
```

Immettere il numero *nnnn* nel campo N. servizio TCP.

Nota: se durante il passaggio di validazione delle tabelle estensioni la configurazione non riesce, la connettività del database può essere un problema. Eseguire di nuovo la configurazione e verificare di aver specificato informazioni corrette sulla connettività del database.

Impostazione del registro di controllo di CA CMDB

Le definizioni di oggetti e trigger, gli attributi e i moduli html utilizzati in CA CMDB per il registro di controllo sono stati modificati all'interno del prodotto.

Per impostare il registro di controllo di CA CMDB r12.5

1. Rimuovere il trigger *cmdb_write_audit_log_site* se è stato creato il file *site/mods/extension.mod* (*extension* specifica il nome dell'estensione).

In questa versione del prodotto il controllo viene creato e abilitato automaticamente.

2. Aggiungere 'UI_INFO("AUDIT_LOG")' a ogni attributo da registrare.
3. Utilizzare i nuovi modelli inclusi nel prodotto per migrare i moduli HTML esistenti.

Nota: per ulteriori informazioni su attributi e moduli HTML, consultare la *Guida all'amministrazione*.

Modalità di integrazione di CA Cohesion ACM con CA CMDB

È possibile integrare CA Cohesion ACM con CA CMDB utilizzando una patch. Contattare il supporto tecnico di CA per ottenere la patch specifica della propria versione di CA CMDB e CA Cohesion ACM.

Configurazione di CA CMDB Visualizer su AIX

Valido su IBM AIX

Per impostazione predefinita, CA Service Desk Manager installa CMDB Visualizer in tutti gli ambienti operativi. Se necessario, è possibile configurare CA CMDB Visualizer. IBM AIX richiede altri file di criteri di protezione.

Per configurare CMDB Visualizer in IBM AIX

1. Verificare che CMDB Visualizer sia configurato.
2. Scaricare file di criteri senza restrizioni (versione 1.4.2 o successiva) dalla relativa pagina nel sito Web di IBM.

Nota: per scaricare i file di criteri è necessario effettuare la registrazione nel sito Web di IBM.

3. Sostituire i file `local_policy.jar` e `US_export_policy.jar` nella directory Shared Components JRE (posizione predefinita: `/opt/CA/SC/JRE/1.6,0/lib/security`) con i file dei criteri scaricati dal sito Web di IBM.
4. Arrestare e avviare Visualizer utilizzando i comandi seguenti:

```
pdm_tomcat_nxd -c STOP -t VIZ  
pdm_tomcat_nxd -c START -t VIZ
```

CMDB Visualizer viene configurato in IBM AIX.

Modifica di script di terze parti per la compatibilità CA CMDB

Per script nella versione corrente del prodotto, l'attributo `ext_asset` viene rinominato con `ID`. Per la compatibilità con CA CMDB con altri prodotti CA che utilizzano l'attributo `ID`, è possibile modificare script di terze parti che utilizzano i servizi web di CA Service Desk Manager per aggiornare le tabelle di estensione di CA CMDB.

Modifica di script di terze parti per CA CMDB

1. Aprire lo script che si desidera modificare.
2. Sostituire tutti i riferimenti SQL di `ext_asset` con `ID`.

Lo script è compatibile con la versione di prodotto corrente.

Modalità di passaggio a un altro server di destinazione per CA CMDB Reports

In genere, un singolo sistema CA Cohesion ACM esporta dati di elementi di configurazione in un unico server CA CMDB per creare report CA CMDB. È possibile passare a un altro server CA CMDB di destinazione per l'esportazione dei dati di elementi di configurazione effettuando le operazioni seguenti:

1. Utilizzare un server CA CMDB come destinazione per l'esportazione dei dati di elementi di configurazione ed eseguire CA CMDB Reports.
2. Riavviare il servizio CA Cohesion ACM Server.
3. Passare a un altro server CA CMDB di destinazione per l'esportazione dei dati di elementi di configurazione ed eseguire CA CMDB Reports.
4. (Facoltativo) Ripetere i passaggi 2 e 3.

Modalità di configurazione dell'interfaccia Web

Quando si installa CA Service Desk Manager, l'*interfaccia Web* (comunemente denominata *interfaccia browser*) viene installata automaticamente ed è possibile configurare l'interfaccia Web come parte dell'installazione. Quando il server Web e il server primario si trovano nello stesso computer, non sono necessarie ulteriori azioni. Tuttavia, se si utilizza un server Web Windows e il server primario è installato in computer diverso, si installeranno e configureranno due server, ovvero un server primario e un server secondario.

Il server secondario è il computer Windows in cui risiede il server Web e in cui si intende installare e configurare l'interfaccia Web. Installare questo server *dopo* avere installato il server primario.

Importante per impostazione predefinita, Tomcat è il server Web predefinito. Se si desidera utilizzare IIS come server Web, configurare manualmente il prodotto e selezionare IIS. Per informazioni, vedere la *Guida in linea della configurazione del server*.

Per configurare l'interfaccia Web, completare la procedura seguente:

1. (Obbligatorio) Abilitare il motore Web sul server secondario.
2. (Obbligatorio) Configurare l'interfaccia Web.

È quindi possibile avviare l'interfaccia Web.

Ulteriori informazioni:

[Abilitazione del motore Web sul server secondario \(Windows\)](#) (a pagina 170)

[Abilitazione del motore Web sul server secondario \(UNIX\)](#) (a pagina 171)

[Configurazione dell'interfaccia Web](#) (a pagina 172)

[Avvio dell'interfaccia Web](#) (a pagina 172)

Abilitazione del motore Web sul server secondario (Windows)

Una volta installato e configurato il server primario CA Service Desk Manager, è necessario abilitare il motore Web sul server secondario.

Per abilitare il motore Web sul server secondario

1. Nel computer in cui è stato installato il server primario, accedere alla directory *directory-installazione\samples\pdmconf*.
2. Utilizzare il comando seguente per avviare l'utilità `pdm_edit`:

```
pdm_perl pdm_edit.pl
```
3. Attenersi alle istruzioni sullo schermo in base alle proprie necessità.
4. Nel menu principale immettere W per selezionare l'opzione di modifica dei motori Web.
5. Immettere A per aggiungere l'host, quindi, immettere l'indirizzo IP o il nome DNS del server secondario quando viene richiesto di specificare un nome host.

Importante poiché questo valore rispetta l'uso delle lettere maiuscole e minuscole, prestare particolare attenzione durante l'inserimento di un nome DNS. In caso di dubbi, controllare la voce `NX_LOCAL_HOST` nel file `NX.env` sul server secondario.

6. Generalmente, quando viene richiesto di specificare un gestore oggetti e un file di configurazione, è possibile accettare i valori predefiniti. Se necessario, modificare i valori.
7. Premere il tasto Invio per tornare al menu principale.
8. Immettere X per creare un file denominato *pdm_startup.rmt* per l'archiviazione dei nuovi valori di configurazione e uscire.
9. Nel computer in cui è installato il server primario, creare un backup del file *pdm_startup.tpl* nella directory *directory-installazione\pdmconf*.
10. Sostituire questo file con il file *pdm_startup.rmt* creato in precedenza.
11. Utilizzare la Configurazione guidata nel server primario senza effettuare cambiamenti, ma configurare il server secondario. Per informazioni, vedere la *Guida in linea della configurazione del server*.

Nota: le nuove impostazioni di configurazione avranno effetto al prossimo avvio del server CA Service Desk Manager.

Abilitazione del motore Web sul server secondario (UNIX)

Una volta installato e configurato il server primario CA Service Desk Manager, è necessario abilitare il motore Web sul server secondario.

Per abilitare il motore Web sul server secondario

1. Nel computer in cui è stato installato il server primario, accedere alla directory `$NX_ROOT/samples/pdmconf`.
2. Utilizzare il comando seguente per avviare l'utilità `pdm_edit`:

```
pdm_perl pdm_edit.pl
```
3. Attenersi alle istruzioni sullo schermo in base alle proprie necessità.
4. Nel menu principale immettere W per selezionare l'opzione di modifica dei motori Web.
5. Immettere A per aggiungere l'host, quindi, immettere l'indirizzo IP o il nome DNS del server secondario quando viene richiesto di specificare un nome host.

Importante poiché questo valore rispetta l'uso delle lettere maiuscole e minuscole, prestare particolare attenzione durante l'inserimento di un nome DNS. In caso di dubbi, controllare la voce `NX_LOCAL_HOST` nel file `NX.env` sul server secondario.

6. Generalmente, quando viene richiesto di specificare un gestore oggetti e un file di configurazione, è possibile accettare i valori predefiniti. Se necessario, modificare i valori.
7. Premere il tasto Invio per tornare al menu principale.
8. Immettere X per creare un file denominato `pdm_startup.rmt` per l'archiviazione dei nuovi valori di configurazione e uscire.
9. Nel computer in cui è installato il server primario creare una copia di backup del file `pdm_startup.tpl` nella directory `$NX_ROOT/pdmconf`.
10. Sostituire questo file con il file `pdm_startup.rmt` creato in precedenza.
11. Utilizzare la Configurazione guidata nel server primario senza effettuare cambiamenti, ma configurare il server secondario. Per informazioni, vedere la *Guida in linea della configurazione del server*.

Nota: le nuove impostazioni di configurazione avranno effetto al prossimo avvio del server CA Service Desk Manager.

Configurazione dell'interfaccia Web

Se la configurazione predefinita specificata per l'interfaccia Web durante l'installazione di CA Service Desk Manager non soddisfa i requisiti, modificare il file *web.cfg*, che si trova nella directory *directory-installazione\bopcfg\www*. Modificare il file utilizzando un editor di testo che non aggiunge caratteri di formattazione o di controllo, come Blocco note o WordPad.

Ciascuna voce nel file è costituita da una riga singola contenente un nome di proprietà, seguito facoltativamente da un valore. Le righe inizianti con un segno di cancelletto (#) vengono considerate come commenti e vengono ignorate.

Nota: per informazioni sulle voci del file *web.cfg*, consultare la *Guida all'amministrazione*.

Avvio dell'interfaccia Web

Prima di avviare l'interfaccia Web e utilizzare CA Service Desk Manager, è necessario verificare che i servizi CA Service Desk Manager Daemon Server e il server del database siano avviati. Se è stato configurato un server secondario (ad esempio, se è installata l'interfaccia Web in un server Web che risiede in un computer diverso dal server primario), è necessario che il servizio Remote Daemon Proctor sia in esecuzione prima di avviare il server primario.

- (Windows) Per avviare i servizi, avviare il Pannello di controllo (Strumenti di amministrazione, Servizi). Fare clic con il pulsante destro del mouse su CA Service Desk Manager Remote Daemon Proctor e scegliere Avvia.
- (Linux) Per avviare i servizi, aprire un prompt dei comandi ed eseguire il comando *pdm_client*.

Dopo avere avviato i servizi, è possibile avviare l'interfaccia Web. La modalità di avvio dell'interfaccia Web dipende dal computer in cui viene eseguita questa operazione, ovvero se si tratta di un server primario o secondario e dall'eventuale utilizzo di IIS. È possibile avviare l'interfaccia Web anche da un sito Web interno.

- Per avviare l'interfaccia Web, selezionare Start, Programmi, CA, Service Desk, Service Desk Web Client.
- Per avviare l'interfaccia Web da un computer che non è il server primario né un server secondario, aprire un browser Web e immettere l'URL seguente:

`http://nomeserver:8080/CAisd/pdmweb.exe`

In questo URL *nomeserver* è il nome del computer che ospita il server Web CA Service Desk Manager.

- Per avviare l'interfaccia Web da un computer che non è il server primario o un server secondario, e come server Web viene utilizzato IIS, aprire un browser Web e immettere l'URL seguente:

`http://nomeserver/CAisd/pdmweb.exe`

- Per avviare l'interfaccia Web da un sito Web interno, aggiungere `/pdmweb.exe` all'URL per le pagine Web. Utilizzare il codice HTML di esempio seguente come guida:

`A HREF=http://<server-name>:<port-no>/CAisd/pdmweb.exe`

In questo URL *nome-server* identifica il computer e *num-porta* è la porta su cui è in ascolto il server Web.

Nota: se la protezione del browser Internet Explorer è impostata su Alta, quando si avvia l'interfaccia Web viene visualizzato un messaggio di avviso. Per evitare che venga visualizzato il messaggio, aggiungere il sito Web all'elenco dei siti affidabili oppure ridurre il livello di protezione di Internet Explorer.

Modalità di configurazione di CA Business Intelligence

Dopo avere installato CA Business Intelligence, è possibile configurarlo per consentirne il corretto funzionamento con CA Service Desk Manager.

1. Configurare le impostazioni iniziali di CA Business Intelligence. Questo passaggio consente di caricare l'universo e i report CA Service Desk Manager, creare gruppi e creare in modo opzionale un utente per ciascun gruppo, oltre a definire autorizzazioni di gruppo.
2. Aggiungere utenti e gruppi CA Service Desk Manager alla console di gestione centralizzata (CMC) di BusinessObjects. Questo passaggio consente di controllare l'accesso dell'utente finale ad InfoView e ad altre applicazioni BusinessObjects.

Nota: per ulteriori informazioni sull'aggiunta di utenti e gruppi e sulla configurazione della sicurezza delle partizioni dati, consultare la *Guida all'amministrazione*.

3. Aggiungere l'account utente CA Service Desk Manager con privilegi predefinito alla CMC.
4. Modificare le impostazioni di protezione e di Web Intelligence predefinite nella CMC.
5. Integrare CA Business Intelligence e CA Service Desk Manager. Questo passaggio consente di specificare le opzioni di report Web in Gestione opzioni.
6. Configurare l'autenticazione sicura per BusinessObjects e CA Service Desk Manager. Il processo di autenticazione consente agli utenti di accedere senza fornire la password più di una volta durante una sessione.

7. (Facoltativo) Configurare l'autenticazione LDAP di BusinessObjects.
8. (Facoltativo) Connettere il server CA Business Intelligence ad un server CA Service Desk Manager diverso.
9. (Facoltativo) Cambiare la dimensione massima di un elenco di valori.
10. (Facoltativo) Modificare i limiti del record del report.
11. (Consigliato) Cambiare il valore di timeout di Web Intelligence.

Configurazione delle impostazioni iniziali di CA Business Intelligence

Dopo avere installato CA Business Intelligence, è necessario completare alcuni passaggi successivi all'installazione e alla configurazione per consentire il corretto funzionamento di CA Business Intelligence con CA Service Desk Manager. Questo passaggio consente di caricare l'universo e i report CA Service Desk Manager, creare gruppi e creare in modo opzionale un utente per ciascun gruppo, oltre a definire autorizzazioni di gruppo.

Per configurare le impostazioni iniziali di CA Business Intelligence

1. Completare il seguente passaggio:
 - Inserire il supporto di installazione nella propria unità. Se il Menu di installazione non viene visualizzato automaticamente, avviare l'installazione facendo doppio clic sul file setup.exe, che si trova nella directory principale del supporto di installazione.

Importante Se il computer non dispone di un'unità appropriata per il supporto di installazione, copiare il contenuto del supporto nel computer in cui si desidera installare CA Business Intelligence. Quindi, avviare la configurazione. Per avviare una configurazione remota in rete, è possibile condividere un'unità o una cartella in rete, quindi connettersi in rete.
2. Selezionare la lingua dall'elenco, quindi fare clic su Seleziona lingua.
Viene visualizzato il menu di installazione.
3. Fare clic sulla scheda Installazione prodotto.
4. Fare clic su Configurazione di CA Business Intelligence.
5. Compilare i campi seguenti della configurazione di CA Business Intelligence.

Nome utente di amministrazione Business Intelligence

Specifica il nome utente di un utente CA Business Intelligence che appartiene al gruppo Amministratori. Il nome utente è l'Amministratore per una nuova installazione di CA Business Intelligence.

Password di amministrazione BI

Specifica la password per l'utente amministrativo di CA Business Intelligence.

Nome utente di amministrazione Service Desk

Specifica il nome utente per l'utente CA Service Desk Manager con privilegi.

Password di amministrazione Service Desk

Specifica la password per l'utente CA Service Desk Manager con privilegi.

Crea Utenti predefiniti

Consente di aggiungere a CA Business Intelligence un set di gruppi CA Service Desk Manager che corrispondono ai ruoli di CA Service Desk Manager. Selezionare questa casella di controllo se si desidera utilizzare un utente di esempio per ciascuno di questi gruppi.

Se CA Business Intelligence è stato installato in un computer diverso da quello in cui è installato CA Service Desk Manager, nella configurazione di CA Business Intelligence vengono visualizzati i campi seguenti:

Host primario Service Desk

Specificare il nome dell'host del server CA Service Desk Manager primario.

Porta ODBC

Specifica il numero di porta del driver ODBC CA Service Desk Manager (è consigliato 1706).

Percorso di installazione ODBC

Specifica il percorso in cui è installato il driver ODBC CA Service Desk Manager.

6. [Verificare](#) (a pagina 176) la configurazione di CA Business Intelligence.
7. (Facoltativo) [Connettere](#) (a pagina 187) il server CA Business Intelligence ad un server CA Service Desk Manager diverso.

Verifica della configurazione di CA Business Intelligence

Dopo avere configurato le impostazioni iniziali, verificare la configurazione di CA Business Intelligence.

Per verificare la corretta configurazione di CA Business Intelligence

1. Avviare InfoView.
2. Accedere con le informazioni seguenti:
 - **System (Sistema)**: specificare il nome host del server in cui è installato CA Business Intelligence.
 - **User name (Nome utente)**: specificare il nome dell'utente amministrativo di CA Business Intelligence (generalmente l'Amministratore).
 - **Password**: specificare la password dell'utente amministrativo di CA Business Intelligence.
 - **Authentication (Autenticazione)**: scegliere il tipo di autenticazione aziendale nell'elenco.
3. Fare clic sull'elenco di documenti ed eseguire le seguenti operazioni:
 - Espandere Public Folders.
 - Espandere CA Reports.
 - Espandere USDK
4. Selezionare la cartella Asset nel riquadro di sinistra.
5. Selezionare il report Asset List.

Il report viene restituito con zero o più risultati trovati.

Importante Se il report non viene eseguito correttamente, o se in InfoView non viene visualizzata la struttura di cartelle precedentemente indicata, è necessario rivedere il registro di configurazione di CA Business Intelligence. Tale file si trova nella directory temporanea dell'utente in una sottocartella denominata BIconfig. Esaminare il file biconfig.log in questa directory per trovare i messaggi di errore. È possibile eseguire nuovamente la configurazione di CA Business Intelligence per risolvere gli errori individuati.

Modalità di configurazione dei valori di intervallo di date e dei parametri di join

Dopo aver installato CA Business Intelligence, effettuare le operazioni seguenti:

- Configurare i valori di intervallo di date in modo che i filtri dell'intervallo di date in CA Business Intelligence funzionino correttamente.
- Configurare i parametri di join in modo che gli outer join dell'universo siano supportati.

Per configurare i valori di intervallo di date e i parametri di join, effettuare le operazioni seguenti:

1. Sul computer in cui è stato installato CA Business Intelligence, passare alla posizione seguente:

```
C:\Programmi\CA\SC\CommonReporting3\BusinessObjects Enterprise  
12,0\win32_x86\dataAccess\connectionServer\odbc\
```

2. Utilizzando un editor di testo, aprire il file `odbc.prm`, passare alla sezione `<Configuration>` e individuare la riga seguente:

```
<Parameter Name="FORMATO_DATA_INPUT_UTENTE">{d 'yyyy-mm-dd'}</Parameter>
```

3. Individuare la riga seguente per configurare i valori di intervallo di date:

```
<Parameter Name="FORMATO_DATA_INPUT_UTENTE">{d 'yyyy-mm-dd'}</Parameter>
```

4. Modificare la riga affinché includa "ore:minuti:secondi (hh:mm:ss)" come illustrato di seguito:

```
<Parameter Name="USER_INPUT_DATE_FORMAT">{d 'yyyy-mm-dd HH:mm:ss am/pm'}</Parameter>
```

5. Individuare la riga seguente per configurare i parametri di join:

```
<Parameter Name="EXT_JOIN">NO </Parameter>
```

6. Modificare la riga sostituendo NO con SÌ, come mostrato di seguito:

```
<Parameter Name="EXT_JOIN">Sì</Parameter>
```

7. Individuare la riga seguente:

```
<Parameter Name="OUTERJOINS_GENERATION">NO</Parameter>
```

8. Modificare la riga sostituendo NO con FULL_ODBC, come mostrato di seguito:

```
<Parameter Name="OUTERJOINS_GENERATION">FULL_ODBC</Parameter>
```

9. Aggiungere le tre righe seguenti dopo il parametro OUTERJOINS_GENERATION:

```
<Parameter Name="LEFT_OUTER"></Parameter> <Parameter Name="RIGHT_OUTER"></Parameter>  
<Parameter Name="OUTERJOINS_COMPLEX">Y</Parameter>
```

10. Salvare il file odbcm.prm.
11. Riavviare i servizi Business Objects Enterprise.

I valori di intervallo di date e i parametri di join sono configurati. I filtri dell'intervallo di date funzionano con CA Business Intelligence e gli outer join dell'universo sono supportati.

Aggiunta di utenti CA Service Desk Manager alla CMC

La CMC è un'utilità di amministrazione che consente di controllare l'accesso degli utenti ad InfoView e ad altre applicazioni BusinessObjects. Con CMC, è possibile assegnare protezione e permessi di accesso utente a cartelle e documenti.

Nota: durante la fase di configurazione, è possibile specificare mediante una casella di controllo facoltativa se devono essere aggiunti utenti di esempio alla CMC. Se è stata selezionata questa opzione, la CMC contiene diversi utenti di esempio. È possibile utilizzare questi campioni come modelli quando si definiscono le autorizzazioni utente e le opzioni di autenticazione per l'ambiente di reporting. Per ulteriori informazioni sugli utenti di esempio, consultare la *Guida all'amministrazione*.

Per aggiungere utenti CA Service Desk Manager alla CMC

1. Dal menù Start sul server CA Business Intelligence, selezionare BusinessObjects XI Release Release 3.1, BusinessObjects Enterprise, BusinessObjects Enterprise Central Management Console.

La CMC Management Console viene visualizzata.

2. Digitare il nome utente e la password con privilegi.
3. Selezionare Enterprise nell'elenco Authentication Type.
4. Fare clic su Accesso.

Viene visualizzata la pagina iniziale della CMC.

5. Fare clic su Users and Groups nella sezione Organize della pagina principale di CMC.

6. Fare clic su Manage (Gestisci), New (Nuovo), New User (Nuovo utente).
Viene visualizzata la finestra di dialogo New User (Nuovo utente).
7. Selezionare Enterprise nell'elenco Authentication Type (Tipo autenticazione).
8. In Account Name (Nome account) specificare l'ID utente di CA Service Desk Manager.
9. Nella scheda Properties specificare le informazioni e le impostazioni relative alla password nel modo seguente:

Password

Immettere la password e confermare. La password immessa dovrebbe corrispondere alla password utente di CA Service Desk Manager. La lunghezza massima per le password è di 64 caratteri.

Questa password deve essere composta da almeno sei caratteri, sia minuscoli che maiuscoli, e non può contenere la parola amministratore o eventuali varianti. La password deve inoltre contenere almeno due dei tipi di carattere seguenti:

- Maiuscolo
- Minuscolo
- Numerico
- Segno di punteggiatura

Password never expires (Nessuna scadenza password)

Selezionare la casella di controllo.

User must change password at next logon (Cambiamento obbligatorio password all'accesso successivo)

Questa casella di controllo è selezionata per impostazione predefinita. Se non si desidera rendere obbligatorio il cambiamento della password al primo accesso, deselezionare la casella di controllo.

10. Per limitare l'accesso ai dati per i report con vincoli di partizione dati o proprietà, selezionare la casella di controllo Enable Data Source Credentials for Business Objects Universes (Abilita credenziali fonte dati per universi Business Objects) . Nei campi che vengono visualizzati specificare il nome e la password dell'account CA Service Desk Manager dell'utente, quindi confermare la password.
11. Fare clic su Actions (Azioni), Members Of (Membri di) per specificare i gruppi cui dovrebbe appartenere l'utente.
12. Fare clic su Join Group (Gruppo di unione) per visualizzare i gruppi disponibili. Per impostazione predefinita, l'utente sarà membro del gruppo Everyone.

13. Nell'area Available groups (Gruppi disponibili) selezionare uno o più gruppi aggiuntivi.
14. Fare clic sulla freccia > per aggiungere i gruppi.
15. Fare clic su OK.

Viene visualizzata la finestra di dialogo Members Of (Membri di) in cui sono elencati i gruppi di cui è membro l'utente.

Nota: per ulteriori informazioni sull'aggiunta di utenti e gruppi e sulla configurazione della sicurezza delle partizioni dati, consultare la *Guida all'amministrazione*.

Aggiungere l'utente privilegiato CA Service Desk Manager a CMC

La connessione all'universo CA Service Desk Manager è configurata per impostazione predefinita per l'utilizzo di utente e password CA Service Desk Manager per l'accesso ai dati. Tale account utente viene aggiunto alla CMC come nuovo utente CA Business Intelligence. Questo utente è necessario se si intende configurare la sicurezza delle partizioni dati, nonché per l'esecuzione delle attività di reporting e del test dei report dalla scheda Report. La scheda Report richiede un utente definito per CA Service Desk Manager e CA Business Intelligence.

Per aggiungere un utente CA Service Desk Manager con privilegi alla CMC

1. Fare clic nell'area di gestione utenti e gruppi della CMC.
2. In Account Name (Nome account) selezionare l'account utente CA Service Desk Manager con privilegi.

3. Nella scheda Properties specificare le informazioni relative alla password.
4. Selezionare la casella di controllo Enable Data Source Credentials for Business Objects Universes (Abilita credenziali fonte dati per universi Business Objects) . Nei campi che vengono visualizzati specificare il nome e la password dell'account dell'utente con privilegi, quindi confermare la password.
5. Fare clic sulla scheda Members Of per specificare il gruppo al quale appartiene l'utente con privilegi.
6. Fare clic su Join Group (Gruppo di unione) per visualizzare i gruppi disponibili.
7. Nell'area Available groups selezionare Administrators e CA Universe Developer.
8. Fare clic sulla freccia > per aggiungere questi gruppi.
9. Fare clic su OK.

Viene visualizzata la finestra di dialogo Member Of in cui sono elencati i gruppi di cui è membro l'utente.

Impostazioni predefinite nella CMC

La maggior parte della configurazione delle funzioni di report viene eseguita automaticamente durante l'installazione di CA Business Intelligence. La configurazione delle funzioni di report comporta le operazioni seguenti:

- Impostazione della sicurezza
- Distribuzione dei report
- Distribuzione degli universi
- Distribuzione degli oggetti del programma
- Configurazione impostazioni di Web Intelligence

L'amministratore può accedere al CMC BusinessObjects e modificare le impostazioni predefinite in qualsiasi momento. L'accesso viene consentito agli utenti in base al gruppo CA Service Desk Manager cui appartengono.

Nota: per ulteriori informazioni su BusinessObjects CMC, consultare la *Guida all'implementazione di CA Business Intelligence*.

Integrazione di CA Business Intelligence con CA Service Desk Manager

Dopo avere installato CA Business Intelligence, aggiornare le opzioni di report Web in modo da consentire la corretta integrazione di CA Service Desk Manager con CA Business Intelligence.

Per integrare CA Business Intelligence e CA Service Desk Manager

1. Nella scheda Amministrazione selezionare Gestione opzioni, Report Web.

Viene visualizzato l'Elenco opzioni.

- Impostare i valori corretti per le opzioni report Web seguenti:

bo_server_auth

Consente di specificare il tipo di autenticazione da utilizzare per il reporting. Si possono specificare i seguenti tipi di autenticazione:

- **secEnterprise.** (Predefinito) Consente di specificare un'autenticazione di tipo aziendale qualora si preferisca creare account e gruppi diversi in BusinessObjects per utilizzarli con CA Business Intelligence o se non è stata impostata una gerarchia di utenti in un database utente Windows NT, un server LDAP o un server Windows AD.

Nota: se si seleziona l'opzione secEnterprise, è necessario aggiungere gli utenti report CA Service Desk Manager alla Console di gestione centralizzata (CMC) di BusinessObjects. Nella CMC immettere gli stessi nomi utente e password configurati in CA Service Desk Manager. Per istruzioni dettagliate, vedere [Aggiunta di utenti CA Service Desk Manager alla CMC](#) (a pagina 178).

- **SecLDAP.** Specificare un'autenticazione LDAP come tipo di autenticazione qualora sia già impostato un server delle directory LDAP e si desideri utilizzare con CA Business Intelligence in BusinessObjects i propri account e gruppi di utenti LDAP di BusinessObjects.

Quando si associano account LDAP a BusinessObjects, gli utenti possono accedere a CA Business Intelligence con il proprio nome utente e password LDAP. In tal modo si evita di creare di nuovi singoli account per utenti e gruppi in BusinessObjects.

- **secWinAD.** Consente di specificare un'autenticazione Windows AD se si lavora in un ambiente Windows 2000 e si desidera utilizzare in CA Business Intelligence gli account esistenti per utenti e gruppi Active Directory di BusinessObjects.
- **secExternal.** Consente di specificare un'autenticazione esterna se si integra la soluzione di autenticazione di BusinessObjects con una di terze parti, ad esempio se si utilizza JCIFS con Tomcat. Questo tipo di autenticazione richiede la configurazione dell'autenticazione sicura in BusinessObjects per consentire agli utenti di accedere senza specificare la propria password.

Nota: per informazioni su opzioni di protezione alternative, vedere la *Guida all'installazione di CA Business Intelligence*.

bo_server_cms

Consente di specificare il nome del CMS (Server di gestione centrale, Central Management Server) responsabile della manutenzione di un database di informazioni sul BusinessObjects che si utilizza con CA Business Intelligence.

Per *bo_hostname*, utilizzare il nome host del computer in cui è installato CA Business Intelligence. Il valore predefinito di *bo_cms_port* è 6400. Per informazioni dettagliate sulle opzioni di configurazione server avanzate, vedere la *Guida all'installazione di CA Business Intelligence*.

bo_server_location

Consente di specificare il valore di *bo_hostname* utilizzando il nome host del computer in cui è installato CA Business Intelligence. CA Service Desk Manager utilizza questo URL per creare gli URL dei report richiesti dal server BusinessObjects. La posizione del CMS è specificata da nome host e porta.

Nota: per informazioni dettagliate su ogni opzione, consultare la *Guida all'implementazione di CA Business Intelligence*.

2. Fare clic su Salva, Aggiorna.

La pagina Dettagli opzioni viene aggiornata con la propria selezione.

3. Fare clic su Chiudi finestra.

4. Fermare e avviare il servizio denominato server CA Service Desk Manager.

Le impostazioni di report Web vengono configurate correttamente per essere utilizzate con CA Service Desk Manager. A questo punto è possibile configurare i report basati sul Web.

Nota: Per informazioni sulla configurazione di report basati sul Web, consultare la *Guida all'amministrazione*.

Modalità di configurazione dell'autenticazione sicura con CA Service Desk Manager e BusinessObjects

L'autenticazione sicura consente di utilizzare un semplice modulo di Single Sign On durante l'integrazione di CA Service Desk Manager e CA Business Intelligence. Single Sign On consente agli utenti di accedere al sistema senza fornire la password più di una volta durante una sessione. Per configurare l'autenticazione sicura tra CA Service Desk Manager e Business Objects, effettuare le operazioni seguenti:

1. Installazione e configurazione di CA Service Desk Manager.
2. Installare e configurare CA Business Intelligence.
3. Accedere alla CMC come amministratore.
4. Accedere alla CMC per impostare l'autenticazione sicura.
5. Creare contatti CA Service Desk Manager e utenti di BusinessObject.
6. Installare le opzioni di report Web di CA Service Desk Manager e impostare l'opzione *bo_server_auth* su Enterprise.
Nota: per ulteriori informazioni su *bo_server_auth*, vedere la *Guida in linea*.
7. Avviare Apache Tomcat BusinessObjects.
8. Quindi riavviare il server CA Service Desk Manager nei servizi Windows.

Configurare l'autenticazione sicura in CA Business Intelligence

Configurare l'autenticazione sicura per CA Business Intelligence richiede innanzitutto la modifica del file web.xml.

Per configurare l'autenticazione sicura in CA Business Intelligence

1. Accedere alla CMC come amministratore.
2. Accedere all'area di gestione dell'autenticazione.
Viene visualizzata la pagina Enterprise.
3. In fondo alla pagina, selezionare l'opzione "Trusted Authentication is enabled", e specificare una stringa di testo nel campo segreto condiviso.
Nota: il segreto condiviso serve per creare una password di autenticazione sicura.
4. Immettere un valore di timeout per le richieste di autenticazione sicura.
Nota: il valore di timeout determina il tempo di attesa di CMS per la chiamata `IEnterpriseSession.logon()` dall'applicazione client.
5. Fare clic su Aggiorna.

6. Modificare il file web.xml dalla cartella di installazione di CA Business Intelligence come segue:

Nota: è possibile localizzare il file nella sottocartella Tomcat55\webapps\OpenDocument\WEB-INF della cartella di installazione di CA Business Intelligence (la cartella di installazione predefinita è C:\Program Files\CA\SC\CommonReporting3).

<param-name>	Valore predefinito	Nuovo valore
param-name	Valore predefinito	Nuovo valore
Opendoc.cms.default	Nome host:porta del CMS	Immettere il nome host e il numero di porta del server CMS BusinessObjects
Opendoc.siteminder.enabled	true	false
Opendoc.sso.enabled	false	true
Opendoc.trusted.auth.user.retrieval	(vuoto)	REMOTE_USER (come specificato dopo la tabella)
Opendoc.trusted.auth.user.param	(vuoto)	(vuoto)
Opndoc.trusted.auth.shared.secret	(vuoto)	(vuoto)

Immettere il parametro *Opendoc.trusted.auth.user.retrieval* come indicato di seguito:

```
<context-param>
  <param-name>Opendoc.trusted.auth.user.retrieval</param-name>
  <param-value>REMOTE_USER</param-value>
</context-param>
```

Nota: non copiare e incollare questo esempio, in quanto potrebbe danneggiare il file web.xml.

Configurare l'autenticazione sicura in CA Service Desk Manager

Configurare l'autenticazione sicura in CA Service Desk Manager richiede la modifica del file TrustedPrincipal.conf.

Per configurare l'autenticazione sicura in CA Service Desk Manager

1. Aprire il file TrustedPrincipal.conf che si trova nella seguente cartella:
NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd
2. Modificare questa riga
SharedSecret=<Segreto condiviso inserito in CMC>

con la seguente stringa:
SharedSecret=xxxx
(dove xxxx è il segreto condiviso inserito nella CMC nel passo 3)
3. Fare clic su Salva.
4. Riavviare il server Tomcat di CA Business Intelligence.

È configurata l'autenticazione sicura in CA Service Desk Manager.

Configurazione dell'autenticazione LDAP di BusinessObjects

Quando si configura l'autenticazione LDAP, il valore "cn" delle credenziali di amministratore del server LDAP deve essere il nome completo (Nome, Cognome). La configurazione dell'autenticazione LDAP consente di riassociare gli attributi LDAP per l'utilizzo del nome di accesso dell'utente.

Importante Il nome account dell'utente di BusinessObjects deve coincidere con l'ID utente di contatto CA Service Desk Manager quando si configura l'autenticazione sicura di LDAP.

Per configurare l'autenticazione LDAP di BusinessObjects

1. Accedere all'area di gestione dell'autenticazione nella Console di gestione centralizzata (CMC).
2. Fare doppio clic su LDAP.

3. Immettere il nome e il numero di porta degli host LDAP nel campo Add LDAP host (Aggiungi host LDAP) (nomehost:porta), ad esempio "mioserver:123".
4. Fare clic su Add (Aggiungi), quindi su OK.
5. Selezionare Custom (Personalizzato) come tipo di server nell'elenco LDAP Server Type (Tipo di server LDAP).
6. Seguire i prompt della configurazione guidata CMS per completare la configurazione.

Nota: per ulteriori informazioni sulla configurazione dell'autenticazione LDAP, vedere la *CMS Online Help* e la *BusinessObjects Enterprise Administrator's Guide*.

Connessione del server di CA Business Intelligence ad un server di CA Service Desk Manager diverso

Dopo aver configurato CA Business Intelligence, non eseguire nuovamente questo processo di configurazione. La configurazione viene utilizzata solo dopo l'installazione iniziale di CA Business Intelligence. Se si desidera connettere questo server CA Business Intelligence ad un server CA Service Desk Manager diverso, effettuare le operazioni seguenti:

1. [Creare un DSN ODBC per il server CA Service Desk Manager](#). (a pagina 187)
2. [Connettere l'universo CA Service Desk Manager a questo server CA Service Desk Manager](#) (a pagina 188).

Creazione di un DSN ODBC per il server CA Service Desk Manager

Utilizzare Amministratore fonte dati ODBC per creare un DSN ODBC.

Per creare un DSN ODBC per il server CA Service Desk Manager

1. Avviare Amministratore fonte dati ODBC (Fonti dati (ODBC)) di Windows.
2. Nel modulo Amministratore fonte dati ODBC selezionare la scheda DSN di sistema e selezionare Aggiungi.
3. Nel modulo Crea nuova fonte dati selezionare il driver DataDirect OpenAccess e selezionare Fine.
4. Nel modulo di impostazione di DataDirect OpenAccess ODBC 32 assegnare un nome ODBC e selezionare Avanzate.

La convenzione di denominazione da utilizzare è casd_hostname. Ad esempio, se il nome host del server CA Service Desk Manager è MyServer, si utilizzerebbe casd_MyServer.

5. Nel modulo di configurazione del database OpenAccess selezionare Aggiungi.
 6. Nel modulo di impostazione del database OpenAccess immettere le informazioni seguenti:
 - **Nome:** specificare casd_hostname.
 - **Indirizzo IP:** specificare l'indirizzo IP del server CA Service Desk Manager.
 - **Porta:** specificare 1706.
 - **Tipo:** selezionare SQL.
 7. Fare clic su OK.
 8. Nel modulo di configurazione del database OpenAccess selezionare OK.
 9. Nel modulo di impostazione di DataDirect OpenAccess ODBC 32, selezionare casd_hostname dall'elenco a discesa Database e fare clic su OK.
- Il DSN ODBC è stato creato.

Connessione dell'universo CA Service Desk Manager al server

Utilizzare Designer in BusinessObjects Enterprise per stabilire una connessione.

Per connettere l'universo CA Service Desk Manager al server CA Service Desk Manager

1. Dal menu Start accedere a BusinessObjects XI Release 2, BusinessObjects Enterprise, Designer.
 2. Accedere a Designer con le credenziali seguenti.
 - **System (Sistema)** - Specificare il nome host del server in cui è stato installato CA Business Intelligence.
 - **User name (Nome utente)** - Specificare il nome dell'utente amministrativo di CA Business Intelligence (generalmente l'Amministratore).
 - **Password** - Specificare la password dell'utente amministrativo di CA Business Intelligence.
 - **Authentication (Autenticazione)** - Selezionare Enterprise.
- Viene visualizzata la finestra Progettazione.

3. Fare clic su File, Import.

Viene visualizzata la finestra di dialogo Import Universe (Importa universo).

4. Selezionare la cartella CA Universes (Universi CA) nell'elenco a discesa, quindi selezionare l'universo CA Service Desk Manager e fare clic su OK.

Nota: se è la prima volta che si utilizza Designer, potrebbe essere necessario fare clic su Browse per selezionare la cartella CA Universes.

5. Fare clic su OK nella casella del messaggio relativo alla corretta importazione dell'universo.

Viene visualizzata la finestra universo.

6. Selezionare File, Parameters.

Viene visualizzata la finestra di dialogo Universe Parameters.

7. Fare clic su Definition nella scheda Edit.

Viene visualizzata la finestra di dialogo Login Parameters (Parametri di accesso).

8. Selezionare Modifica.

9. Selezionare l'ODBC DSN creato (casd_hostname) nell'elenco a discesa dei nomi fonte dati e specificare l'utente e la password CA Service Desk Manager con privilegi.

10. Fare clic su Next, Test Connection e seguire le istruzioni nelle finestre di dialogo visualizzate per la connessione dell'universo.

11. Per terminare l'operazione, fare clic su OK.

12. Selezionare File, Export.

Viene visualizzata la finestra di dialogo Esporta Universo.

13. Selezionare /CA Universes (Universi/CA) nell'elenco a discesa Domain (Dominio).

14. Selezionare Everyone dall'elenco Groups.

15. Fare clic su OK.

Viene esportato l'universo e viene stabilita la connessione al server.

Cambiamento della dimensione massima di un elenco di valori

Quando si installa CA Business Intelligence, il numero massimo di valori che possono essere restituiti in batch per un elenco di valori nei report Crystal è impostato automaticamente su 5.000 record dal database. Per motivi di prestazioni, è possibile cambiare le dimensioni in modo che l'elenco di valori venga restituito all'utente in diversi batch della dimensione indicata o di una dimensione inferiore.

Nota: per informazioni sul miglioramento delle prestazioni di Web Intelligence Report Server, consultare la documentazione di BusinessObjects.

Per cambiare la dimensione massima di un elenco di valori

1. Avviare l'editor del Registro di sistema.
2. Nella struttura espandere HKEY_CURRENT_USER, Software, Business Objects, Suite 11.0, Crystal Reports, Database.
3. Creare una chiave del Registro di sistema denominata QPMaxLOVSize.
4. Selezionare Nuovo, Valore DWORD.
5. Nel campo Nome inserire DWORD.
6. Nella finestra di dialogo Modifica valore DWORD immettere 1000 nel campo Valore e fare clic su OK.
7. Selezionare File, Esci per chiudere l'editor del Registro di sistema.
8. Utilizzando BusinessObjects Enterprise, effettuare l'accesso alla Console di gestione centralizzata.
9. Passare alle impostazioni delle proprietà di Web Intelligence Report Server.
10. Impostare le opzioni relative alla *dimensione batch dell'elenco valori* e alla *dimensione massima dell'elenco valori per l'ordinamento personalizzato* su 1000 o su un valore appropriato ai requisiti specifici.
11. Salvare le impostazioni.

La dimensione massima viene cambiata e utilizzata per la restituzione di un elenco di valori.

Cambiamento dei limiti del record del report

Quando si installa CA Business Intelligence, il numero di record che il server recupera dal database quando un utente esegue una query o un report in Crystal Reports è impostato automaticamente su 20.000 record. È possibile cambiare l'impostazione per consentire agli utenti che eseguono report di ricevere i set di record previsti.

Nota: per i dettagli completi sulle attività amministrative che è possibile completare per Crystal Reports Page Server, consultare la documentazione di BusinessObjects.

Per modificare i limiti del record del report

1. Utilizzando BusinessObjects Enterprise, effettuare l'accesso alla Console di gestione centralizzata.
2. Passare alla pagina in cui sono visualizzati i server.
3. Fare clic su Crystal Reports Page Server (Pagina del server Crystal reports).
4. Nella scheda Properties (Proprietà) cambiare l'impostazione per il campo *Database Records To Read When Previewing or Refreshing a Report* (Record di database da leggere durante l'anteprima o l'aggiornamento di un report) specificando un numero di record illimitato oppure un limite di record specifico.
5. Fare clic su Applica.
6. Riavviare Crystal Reports Page Server.

Il limite del record di report cambia e viene utilizzato per l'esecuzione di report.

Cambiamento del valore di timeout della sessione di Web Intelligence

Gli utenti dispongono dei diritti di accesso con controllo completo all'applicazione Web Intelligence per impostazione predefinita.

Il timeout di sessione predefinito per l'applicazione Web Intelligence è 20 minuti. I report non salvati vengono persi quando si verifica il timeout della sessione e l'utente deve eseguire un nuovo accesso per utilizzare l'applicazione.

Gli amministratori possono modificare il valore di timeout della sessione di connessione utilizzando la Console di gestione centralizzata (CMC).

Per cambiare il valore di timeout della sessione di Web Intelligence

1. Selezionare Server nella pagina iniziale di CMC.
Viene visualizzata la finestra Server
2. Selezionare Web_IntelligenceReportServer nella colonna Nome server.
3. Digitare il valore di timeout appropriato (numero di minuti) nel campo Timeout connessione.
4. Fare clic su Applica.
I cambiamenti saranno effettivi una volta riavviato il server.
5. Fare clic su OK
Viene impostato il valore di time-out della sessione.

Database replicato per il reporting non in linea

Per gestire i possibili problemi di prestazioni che potrebbero interessare i componenti di reporting installati con CA Service Desk Manager, è possibile creare un database replicato in modo da poterlo utilizzare per il reporting non in linea.

Nota: per ulteriori informazioni sulla creazione di un database replicato per il reporting non in linea, consultare la documentazione e gli script di esempio contenuti nella directory NX_ROOT\samples\reporting.

Esecuzione delle Norme automatiche

La funzionalità Norme automatiche di Gestione delle informazioni offre una serie di norme automatiche che consentono di gestire la conoscenza dell'organizzazione in modo più efficace ed efficiente. Una norma automatica descrive la condizione per cui i documenti vengono contrassegnati per la correzione e promossi per la pubblicazione o il ritiro attraverso le varie fasi del processo del ciclo di vita del documento. Ad esempio, è possibile specificare la norma predefinita "correzione collegamenti interrotti" che corrisponde ai documenti trovati nell'archivio della conoscenza con collegamenti interrotti. Il compito di correzione di un problema può essere assegnato ad un analista.

Nella pagina Elenco norme automatiche sono inclusi i dettagli relativi alle norme che è possibile gestire. Per visualizzare tale pagina, selezionare la scheda Amministrazione, Conoscenza, Norme automatiche.

Ogni norma include una query memorizzata che viene eseguita quando vengono messi in corrispondenza i documenti durante l'elaborazione. Dopo l'elaborazione, viene visualizzato un report relativo alle norme del ciclo di vita nel contatore CA Service Desk Manager. Per visualizzare un report, selezionare Documenti della conoscenza, Norme automatiche. Dal contatore l'analista può gestire i propri documenti e, per impostazione predefinita, l'amministratore può gestire tutti i documenti per ciascun ruolo.

Per implementare i report, è necessario eseguire un processo in batch mediante Automated Policies Scheduler. Il pianificatore viene eseguito sul server e vengono visualizzati i dati richiesti per visualizzare i report. Al termine, eseguire la [scheda Report della conoscenza](#) (a pagina 194).

Per eseguire Automated Policies Scheduler

1. Fare clic sulla scheda Amministrazione, quindi accedere a Conoscenza, Norme automatiche, Pianificazione.

Viene visualizzato Automated Policies Scheduler.

2. Inserire i dati nei seguenti campi:

Ultimo aggiornamento

Selezionare la casella di controllo Esegui calcolo.

Pianifica

Specificare una data e un'ora in cui CA Service Desk Manager inizierà ad eseguire il calcolo e ad eseguire le norme.

3. Fare clic su Salva.

Esecuzione della scheda Report della conoscenza

Per eseguire la scheda Report della conoscenza

1. Fare clic sulla scheda Amministrazione.
2. Accedere a Conoscenza, Scheda report della conoscenza.
Viene visualizzata la Scheda report della conoscenza.
3. Inserire i dati nei seguenti campi:

Ultimo aggiornamento

Selezionare la casella di controllo Esegui calcolo.

Pianifica

Specificare una data e un'ora in cui CA Service Desk Manager inizierà ad eseguire il calcolo e ad eseguire le norme.

4. Fare clic su Salva.

Nota: per informazioni sull'utilizzo delle Norme automatiche e della scheda Report della conoscenza, consultare la *Guida all'amministrazione di Gestione delle informazioni*.

Importazione di dati di esempio di Gestione delle informazioni

È possibile utilizzare i dati della conoscenza di esempio provenienti da Knowledge Broker e Knowledge Accelerators. Per utilizzare tali dati, è necessario importarli nel database di Gestione delle informazioni. A tale scopo, attenersi alle istruzioni riportate di seguito.

Installazione di Windows

1. Spostarsi sulla directory `$NX_ROOT\samples\data` e decomprimere il file `SampleData.zip` nella stessa directory.
2. Dalla finestra dei comandi passare a `$NX_ROOT/bin` ed eseguire `ImportSampleData.bat`.

Installazione di UNIX

1. Eseguire il comando `tar -xvf SampleData.tar` da `$NX_ROOT/samples/data`.
2. Dalla finestra dei comandi passare a `$NX_ROOT/bin` ed eseguire `ImportSampleData.sh`.

Modalità di configurazione di FAST ESP

Dopo avere installato FAST ESP, effettuare i passaggi seguenti per configurare FAST ESP in modo da consentirne il corretto funzionamento con CA Service Desk Manager:

1. (Obbligatorio) Specificare se si desidera utilizzare il motore del modulo di ricerca FAST ESP.
2. Configurare le funzionalità di ricerca e indicizzazione per i repository esterni (siti Web e directory locali).
3. Cambiare la strategia di lemmatizzazione per una lingua.
4. Configurare i sinonimi.
5. Aumentare le funzionalità della ricerca FAST ESP.
6. Eseguire il backup dei dati di FAST ESP
7. Integrare FAST ESP in un server secondario.

Importante Se per qualsiasi motivo si arrestano e si riavviano i servizi FAST ESP, è *necessario* arrestare e riavviare anche il daemon di indicizzazione (bpeid_nxd). Per consentire l'avvio del daemon, è *necessario* che FAST ESP sia in esecuzione. In caso contrario, verranno visualizzati errori in *stdlog* e alla creazione o ricerca di documenti della conoscenza.

Nota: per informazioni dettagliate sulla configurazione, vedere *FAST ESP Configuration Guide*.

Ulteriori informazioni:

[Utilizzo del motore di ricerca FAST](#) (a pagina 196)

[Ricerca in repository esterni](#) (a pagina 197)

[Cambiamento della strategia di lemmatizzazione](#) (a pagina 200)

[Configurazione dei sinonimi](#) (a pagina 203)

[Ricerche Argomenti correlati](#) (a pagina 204)

[pdm_k_reindex—Utilità di reindicizzazione della conoscenza](#) (a pagina 205)

[Utilizzo di pdm_k_reindex con FAST ESP](#) (a pagina 206)

[Aumento delle capacità di ricerca](#) (a pagina 208)

[Modalità di esecuzione del backup dei dati di FAST ESP](#) (a pagina 208)

[Integrazione di FAST ESP nel server secondario](#) (a pagina 209)

Utilizzo del motore di ricerca FAST

Per impostazione predefinita, CA Service Desk Manager è configurato per l'utilizzo del motore di ricerca Gestione delle informazioni. Se è installato il motore di ricerca FAST ESP, è possibile impostarlo come predefinito per eseguire le ricerche in Gestione delle informazioni. Completare i passaggi seguenti sul server CA Service Desk Manager primario o secondario.

Per utilizzare il motore di ricerca FAST

1. Fare clic sulla scheda Amministrazione.
Viene visualizzata la console di amministrazione.
2. Nella struttura a sinistra, fare clic su Gestione opzioni, Motore di ricerca.
Viene visualizzato l'Elenco opzioni.
3. Specificare le impostazioni seguenti:

ebr_version

Specificare FAST [Motore di ricerca].

ebr_search_engine_baseport

Specificare la porta di base del server dedicato nel quale è installato il motore del modulo di ricerca FAST ESP. Prendere in considerazione quanto segue quando si specifica la porta di base:

- Assicurarsi che il numero di porta immesso qua corrisponda alla porta di base specificata durante l'installazione di FAST ESP (la porta predefinita è 13000).
- La porta di base viene utilizzata da FAST ESP per calcolare le porte statiche.
- In ciascun host è necessario che sia presente una serie di 4000 porte tra la porta di base FAST ESP e l'installazione FAST ESP perché FAST ESP sposta le porte statiche dalla porta di base (ovvero, il numero di porta dell'interfaccia di amministrazione se è 16000).
- Assicurarsi che questo intervallo di porte non confligga con altri prodotti o servizi utilizzati dal server.
- Non è possibile utilizzare porte sotto la 1024.
- È consigliato di *non* usare una porta di base nella serie da 23000 a 27000, poiché il server delle licenze utilizza sempre il numero di porta 27000.

Importante tutti gli host devono possedere l'accesso illimitato alla rete per l'intero intervallo di porte (ad esempio, le porte da 13000 a 16999).

ebr_search_engine_host

Specificare il nome di dominio qualificato o l'indirizzo IP (consigliato) del server dedicato sul quale è installato il motore del modulo di ricerca FAST ESP.

4. Fare clic su Salva, Aggiorna.

La pagina dei dettagli delle opzioni viene aggiornata con la propria selezione.

5. Fare clic su Chiudi finestra.
6. Fermare e avviare il servizio denominato server CA Service Desk Manager.
7. Eseguire il comando *pdm_k_reindex index factory:all* per indicizzare documenti della conoscenza e ticket in FAST ESP.

Nota: per informazioni su come eseguire il comando *pdm_k_reindex*, consultare la *Guida all'amministrazione*.

Ricerca in repository esterni

Dalla pagina Ricerca della conoscenza o dalla scheda Conoscenza in un ticket Service Desk, analisti e gestori della conoscenza possono recuperare contenuti non strutturati da repository esterni (siti Web e file system) selezionando la fonte dati Repository esterni nell'elenco Tipo della conoscenza. Gli utenti possono recuperare il contenuto dei repository esterni raccolto dalle directory locali, da Internet o da una rete Intranet.

Importante Dopo l'installazione di FAST ESP e CA Service Desk Manager, non sono necessari passaggi aggiuntivi per la configurazione della ricerca e dell'indicizzazione per i documenti della conoscenza, i forum, i file della conoscenza e i ticket di Service Desk. Per impostazione predefinita, questo contenuto viene recuperato, elaborato, abilitato per le ricerche, quindi raggruppato nella raccolta *kd* predefinita nell'interfaccia di amministrazione di FAST ESP.

In FAST ESP è possibile utilizzare uno o entrambi i metodi seguenti per configurare la ricerca e l'indicizzazione per i siti Web e le directory locali:

- [Aggiunta di repository esterni per ricerche in siti Web](#) (a pagina 198)
- [Aggiunta di repository esterni per directory locali](#) (a pagina 200)

Importante il contratto di licenza predefinito per eseguire ricerche con il modulo di ricerca FAST ESP specifica le seguenti limitazioni: due ricerche al secondo e due milioni di oggetti indicizzati. A causa di queste limitazioni, è consigliabile non aggiungere siti Web di grandi dimensioni come ca.com. Si consiglia inoltre di non cambiare i parametri relativi alla frequenza delle richieste e all'intervallo di aggiornamento se non esiste un motivo specifico per farlo.

Aggiunta di repository esterni per ricerche in siti Web

È possibile utilizzare l'interfaccia di amministrazione di FAST ESP per aggiungere un set di URI da cui iniziare l'esplorazione del Web. Ad esempio, <http://www.my-site-to-index.com>. Enterprise Crawler connette la raccolta di URI definita dall'utente ad un agente di ricerca Web per il recupero del contenuto.

Nota: alcuni siti Web bloccano la funzionalità di ricerca per indicizzazione delle applicazioni. Per ulteriori informazioni sulla risoluzione dei problemi di Enterprise Crawler, vedere la FAST ESP Enterprise Crawler Guide, che si trova in `\CA_tps.nt\FastESP\Doc\en-US`.

Effettuare le seguenti operazioni sul computer in cui è installato il motore del modulo di ricerca FAST ESP.

Per aggiungere repository esterni per ricerche in siti Web

1. Avviare l'interfaccia di amministrazione di FAST ESP dal browser Web.
 - Presupponendo che sia stata mantenuta l'impostazione di installazione predefinita (13000) per l'intervallo di porte di base FAST, è possibile immettere l'interfaccia di amministrazione all'indirizzo *<http://machinename:16000>*, in cui il numero di porta è la porta base + 3000.
 - Se si cambia l'intervallo predefinito della porta di base, è possibile accedere all'interfaccia amministrativa di FAST ESP all'indirizzo *<http://machinename:default start port range + 3000/>*.
2. Per accedere a FAST Home per la prima volta come amministratore, utilizzare Admin come nome utente e lasciare vuoto il campo della password. Passare quindi a FAST Home, User Administration (Amministrazione utente), Create Users & Groups (Crea utenti e gruppi) per immettere una nuova password per l'account admin.
3. Dalla home page fare clic sul collegamento ESP Admin GUI a destra.

Nota: il collegamento ESP Admin GUI avvia l'interfaccia di amministrazione di FAST ESP. È possibile ignorare il collegamento Clarity che avvia lo strumento di monitoraggio di FAST. Per ulteriori informazioni su questi collegamenti, vedere *FAST Operations Guide*.

Viene visualizzata la pagina Collection Overview (Panoramica raccolta).

4. Dalla raccolta di *siti* selezionare l'icona Edit (Modifica) visualizzata nella colonna Docs.

Viene visualizzata la pagina Collection Details (Dettagli raccolta).

5. Dal Control Panel (Pannello di controllo) fare clic sull'icona Edit Data Sources (Modifica fonti dati).

Viene visualizzata la pagina Edit Collection (Modifica raccolta).

6. Nell'elenco Available Data Sources (Fonti dati disponibili) selezionare Enterprise Crawler (Agente di ricerca Enterprise).

Enterprise Crawler connette la raccolta ad un agente di ricerca Web per il recupero del contenuto.

7. Fare clic sul pulsante che consente di *aggiungere gli elementi selezionati*.

Viene visualizzata la pagina di impostazione Edit Collection (Modifica raccolta), New Data Source (Nuova fonte dati).

Nota: i parametri relativi alla frequenza delle richieste e all'intervallo di aggiornamento definiscono la frequenza con cui l'agente di ricerca visita i server Web del dominio Web indicato.

8. Immettere un URI di avvio nella casella Start URI (Avvia URI), come mostrato. Il campo Start URI consente di aggiungere un set di URI da cui avviare la ricerca (ad esempio, <http://www.my-site-to-index.com>). Per consentire l'avvio della ricerca, è necessario definire almeno un URI (o un file contenente un elenco di URI). Accertarsi che l'URI termini con una barra (/). Non è possibile aggiungere due volte lo stesso URI.

- a. Fare clic sull'icona freccia di aggiunta per aggiungere l'URI al set di URI nella casella di testo a destra.

Per rimuovere un URI di avvio dall'elenco, evidenziarlo e fare clic sull'icona freccia di rimozione.

Per impostazione predefinita viene contemporaneamente aggiunto un *filtro di inclusione del nome host esatto* all'elenco degli host consentiti nel campo Hostname include filters (Filtri inclusione nome host). Verrà eseguita la ricerca in tutti i server di www.mysitename.com host.

- b. Fare clic su Invia.

Attendere alcuni minuti, quindi rivedere il conteggio dei documenti indicizzati per verificare l'avanzamento dell'indicizzazione.

9. Fare clic su OK.

Ora è possibile eseguire ricerche dalla fonte dati dei repository esterni nella pagina Ricerca della conoscenza o dalla scheda Conoscenza in un ticket Service Desk.

Aggiunta di repository esterni per directory locali

È possibile utilizzare ESP File Traverser per recuperare i file dalle directory nei server di file e inoltrarli in una raccolta specificata per consentirne l'ulteriore elaborazione.

Nota: per i dettagli completi sui comandi di *filetraverser*, vedere la ESP File Traverser Guide, che si trova in \CA_tps.nt\FastESP\Doc\en-US.

Effettuare le seguenti operazioni sul computer in cui è installato il motore del modulo di ricerca FAST ESP.

Per aggiungere repository esterni per le directory locali

1. Aprire una finestra del prompt dei comandi e utilizzare il comando *filetraverser* per indicizzare una directory che contiene file HTML da indicizzare.

Il comando utilizzato per eseguire File Traverser potrebbe avere aspetto simile al seguente:

```
filetraverser -r C:\HTML -s html -c site -p http://test03.ca.com/test
```

Nota: in questo esempio i file HTML vengono indicizzati dalla directory *C:\test* nel sito della raccolta quando viene assegnato il prefisso *http://test.my-files.com/test* a tutte le pagine.

2. Attendere alcuni minuti, quindi rivedere il conteggio dei documenti indicizzati nella pagina Collection Overview nell'interfaccia di amministrazione di ESP per verificare il completamento dell'indicizzazione.

Ora è possibile eseguire ricerche dalla fonte dati dei repository esterni nella pagina Ricerca della conoscenza o dalla scheda Conoscenza in un ticket Service Desk.

Cambiamento della strategia di lemmatizzazione

In CA Service Desk Manager è possibile specificare la lingua delle query impostando la variabile *NX_EBR_QUERY_LANGUAGE* nel file *\$NX_ROOT\NX.env*. Per impostazione predefinita, non è richiesta nessuna variabile. È necessario definire questa variabile per il cinese, il giapponese e il coreano.

Considerare le informazioni riportate di seguito quando si cambia la strategia di lemmatizzazione e si specifica la lingua di query:

Importante per dettagli completi sul cambiamento della strategia di lemmatizzazione, consultare la documentazione di FAST ESP disponibile sui supporti di installazione, compresi i documenti *FAST ESP Advanced Linguistics Guide*, *FAST ESP Troubleshooting Guide* e *FAST ESP Query Language Parameters Guide*. Inoltre, se si configura una nuova lingua o si cambia la strategia di lemmatizzazione, occorre rielaborare tutti i documenti indicizzati.

- In CA Service Desk Manager è disponibile il supporto linguistico per le query all'interno di FAST ESP per le lingue seguenti:

Gruppo	Lingue supportate
1	■ Inglese (en) ■ Francese (fr) ■ Tedesco (de) ■ Giapponese (ja)
2	■ Italiano (it) ■ Cinese semplificato (zh semplificato) ■ Spagnolo (es) ■ Portoghese brasiliano (pt)
3	■ Coreano (ko) ■ Cinese tradizionale (zh tradizionale) ■ Tailandese (th)

- Quando si installa FAST ESP come parte dell'installazione di CA Service Desk Manager, non è possibile specificare il supporto per più lingue. Per utilizzare il supporto per più lingue, è necessario distribuire il file *LemmatizationConfig.xml* (che si trova nella directory \$FASTSEARCH/etc) che definisce la strategia di lemmatizzazione per tutte le lingue supportate.

In questo file *LemmatizationConfig.xml* sarà incluso un elenco di tutte le lingue con supporto linguistico avanzato in InStream 5.1.3, incluse le lingue seguenti:

■ Olandese	■ Tedesco	■ Coreano
■ Arabo	■ Estone	■ Ungherese
■ Polacco	■ Slovacco	■ Ucraino
■ Inglese	■ Italiano	■ Norvegese
■ Ceco	■ Finlandese	■ Hindi
■ Rumeno	■ Svedese	■ Portoghese
■ Francese	■ Giapponese	■ Lettone
■ Danese	■ Ebraico	■ Spagnolo
■ Russo	■ Turco	■ Lituano

Nota: per tutte le altre lingue non sarà disponibile il supporto linguistico avanzato.

- Per alcune lingue è possibile indicizzare il contenuto ed eseguire le ricerche solo con un'elaborazione linguistica specializzata. Tali lingue includono il cinese, il giapponese, il coreano e il thailandese. In FAST ESP sia i documenti da indicizzare che le query vengono sottoposti ad elaborazione linguistica, gran parte della quale è specifica della lingua.
- FAST ESP è in grado di identificare automaticamente la lingua di ciascun documento inviato per l'indicizzazione. Tuttavia, dal momento che molte lingue condividono gli stessi script o script analoghi, le query di ricerca sono generalmente troppo brevi per consentire un'accurata identificazione della lingua. Pertanto, è importante che la lingua di una query sia specificata per impostazione predefinita oppure venga specificata quando vengono inoltrate le singole query. In caso contrario, la query potrebbe essere elaborata in modo non corretto.

Esempio: identificare i documenti brevi in base alla lingua e abilitarli alla ricerca

Nota: in questo esempio viene illustrato come identificare documenti brevi in giapponese e come abilitarli per la ricerca in FAST ESP. È inoltre possibile identificare documenti brevi in cinese e coreano.

È possibile imporre la lingua nella pipeline di CA Service Desk Manager (webcluster) fintantoché vengono definiti i criteri appropriati.

Se nella raccolta di FAST ESP vengono inseriti tutti i documenti giapponesi, è possibile imporre la lingua utilizzando un tipo di fase AttributeAssigner oppure è possibile configurare la lingua utilizzando il parametro FallbackLanguage della fase LanguageAndEncodingDetector.

Se la raccolta di FAST ESP contiene documenti in giapponese e in altre lingue, occorre definire dei criteri, ad esempio basati su ID, per determinare la lingua. Pertanto è necessario creare una fase personalizzata per implementare tali criteri e assegnare la lingua corretta.

È inoltre possibile assegnare una lingua dalla posizione di origine dei documenti, ad esempio il database, l'agente di ricerca o un altro meccanismo di estrazione. Se la lingua è già nota nella fase di estrazione, può essere trasferita nella pipeline e rimanere inalterata mediante la disabilitazione del rilevamento della lingua.

Configurazione dei sinonimi

Quando si utilizzano i *sinonimi* con FAST ESP, è possibile eseguire la ricerca del contenuto rilevante e trovarlo, anche se non include nessuno dei termini o delle espressioni utilizzati per la ricerca. Se ad esempio si definisce il sinonimo *musica* per i termini mp3 e mp4, cercando la parola musica, sarà possibile trovare i documenti contenenti il termine mp3 o mp4. È inoltre possibile utilizzare i sinonimi per riscrivere un termine e visualizzare solo i risultati che si ritengono più appropriati per l'azienda. Ad esempio è possibile riscrivere il termine *laptop* in modo che vengano restituiti solo i risultati relativi ad un modello specifico di laptop.

Nota: per i dettagli completi e le procedure di gestione dei sinonimi, consultare il manuale *FAST ESP Search Business Center Guide*.

Per configurare i sinonimi

1. Accedere al LinguisticsStudio FAST ESP servendosi delle istruzioni fornite nella documentazione di FAST ESP.
2. Utilizzare LinguisticsStudio per completare la procedura seguente:
 - a. Creare un progetto di linguistica.
 - b. Creare un dizionario e denominarlo *casynonyms*.
 - c. Aggiungere nuovi sinonimi al dizionario. Ad esempio, musica per i termini mp3 ed mp4.

Viene creato il nuovo file di dizionario seguente:

`$FASTROOT\resources\dictionaries\synonyms\qt\casynonyms.aut`

- d. Aggiungere la voce seguente al nuovo dizionario nel file `$FASTROOT\etc\config_data\QRServer\webcluster\etc\qrserver\qtf-config.xml`:

```
<instance name="synonym" type="external" resource="qt_synonym">
<parameter-list name="qt.synonym">
<parameter name="enable" value="1"/>
<parameter name="synonymdict1" value="resources/dictionaries/synonyms/qt/short_spellvars.aut"/>
<parameter name="synonymdict2" value="resources/dictionaries/synonyms/qt/short_wordnet.aut"/>
<parameter name="synonymdict3" value="resources/dictionaries/synonyms/qt/casynonyms.aut"/>
</parameter-list>
</instance>
```

3. Arrestare il servizio *qrserver*.
4. Distribuire il nuovo file di dizionario in FAST ESP.
5. Avviare il servizio *qrserver*.
6. Eseguire il comando *setupenv.cmd* nella directory `$FASTROOT\bin`.
7. Eseguire il comando *view-admin.cmd -a -m refresh* nella directory `$FASTROOT\bin`.
8. Aggiornare *NX.env* con `@NX_EBR_QUERY_WITH_SYNONYMS=Yes`.
9. Riavviare CA Service Desk Manager.

Ulteriori informazioni:

[Installazione di LinguisticsStudio](#) (a pagina 156)

Ulteriori informazioni:

[pdm k reindex—Utilità di reindicizzazione della conoscenza](#) (a pagina 205)
[Utilizzo di pdm k reindex con FAST ESP](#) (a pagina 206)

Ricerche Argomenti correlati

È possibile ricercare ticket simili, comprese questioni, richieste, incidenti, problemi e ordini di cambiamento, utilizzando la scheda Conoscenza dei ticket. Argomenti correlati è attivo solo quando si installa FAST ESP. Questa funzionalità consente di ricercare ticket simili utilizzando il riepilogo del ticket e la descrizione come query di ricerca. La ricerca di ticket simili evita che sia necessario creare ticket ridondanti nell'ambiente di supporto.

Importante Per usare Argomenti correlati, è necessario eseguire [pdm k reindex](#) (a pagina 206) per sincronizzare i documenti. È inoltre necessario reindicizzare ciascuno degli oggetti CA Service Desk Manager, come le richieste di chiamate, gli ordini di cambiamento e così via.

pdm_k_reindex—Utilità di reindicizzazione della conoscenza

L'utilità di reindicizzazione della conoscenza, `pdm_k_reindex.exe`, si trova nella directory di installazione di Gestione delle informazioni. È possibile usare questa utilità anche in un'[integrazione FAST ESP](#) (a pagina 206).

Nota: la reindicizzazione dei documenti dell'archivio della conoscenza può richiedere molto tempo, a seconda delle dimensioni del database. Pertanto, si consiglia di eseguire l'utilità Knowledge Reindex solo dopo aver apportato tutti i cambiamenti.

Per eseguire l'utilità Knowledge Reindex, immettere il comando seguente al prompt dei comandi:

```
pdm_k_reindex
```

Di seguito sono riportate le opzioni disponibili con questo comando.

Interfaccia:

-D

Definisce la modalità di debug, ad esempio la stampa sulla finestra di comando.

-v

Definisce la modalità dettagliata, ad esempio la stampa nel file `stdlog`.

-i

Non crea gli indici di tabella nella tabella di reindicizzazione dopo l'esecuzione della reindicizzazione.

Nota: i parametri il cui prefisso contiene un trattino, ad esempio "-D", devono precedere gli altri parametri.

file:reindex.txt

I documenti vengono reindicizzati nel file appropriato.

+i

Crea solo gli indici della tabella di reindicizzazione, che diventerà la tabella di ricerca dopo l'esecuzione della reindicizzazione. I vecchi indici verranno eliminati prima del processo di reindicizzazione.

+t

Cambia solo i nomi della tabella di ricerca e della tabella di reindicizzazione.

Nota: il prefisso "+" indica che verrà applicato solo il parametro ad esso associato.

sdtout

Consente di specificare la frequenza con cui vengono visualizzate le informazioni statistiche nella finestra del comando. Per impostazione predefinita, l'utilità Knowledge Reindex fornisce informazioni statistiche nella finestra di comando ogni 1000 documenti elaborati. Talvolta, tuttavia, viene richiesto di fornire le statistiche con maggiore frequenza. Utilizzare il parametro:

```
pdm_k_reindex -i sdtout:10
```

In questo caso, le statistiche vengono visualizzate nella finestra di comando dopo l'elaborazione di dieci documenti.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA Service Desk Manager. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

Utilizzo di pdm_k_reindex con FAST ESP

L'utilità pdm_k_reindex viene impiegata per reindicizzare, deindicizzare e sincronizzare (reindicizzazione e deindicizzazione) factory di documento: DC, R, Q, ecc. L'utilità viene richiamata nel modo seguente:

```
pdm_k_reindex [operation] [factory] [mode]
```

operazione

Sono valide le seguenti operazioni:

-h

Visualizza la Guida in linea dell'utilità.

indicizzazione

(Impostazione predefinita) Reindicizza i documenti.

deindicizzazione

Deindicizza i documenti.

sincronizzazione

Consente di reindicizzare e/o deindicizzare i documenti per sincronizzare il motore di ricerca dopo l'esecuzione di un'operazione di eliminazione o ripristino. È possibile utilizzare le seguenti modalità per la sincronizzazione:

- **eliminazione**

Sincronizza il motore di ricerca dopo un'operazione di eliminazione.

- **ripristino**

Sincronizza il motore di ricerca dopo un'operazione di ripristino.

status

Visualizza il numero restante di documenti da elaborare.

factory

Sono valide le seguenti factory:

tutte

Imposta tutte le factory.

DC

(Predefinito) Definisce la factory DC.

cr

Imposta la factory cr.

iss

Imposta la factory iss.

modalità

Sono valide le seguenti modalità:

eliminazione

Sincronizza il motore di ricerca dopo un'operazione di eliminazione.

ripristino

Sincronizza il motore di ricerca dopo un'operazione di ripristino.

Nota: se non si selezionano argomenti factory, la factory DC non viene indicizzata.

Esempi di parametri di indicizzazione

```
pdm_k_reindex [index] [factory:KD|cr|iss|all]
```

Esempio di parametri di deindicizzazione

```
pdm_k_reindex deindex factory:KD|cr|iss|all [clearrange]
```

clearrange

(Opzionale) Deindicizza i documenti che non rientrano nell'intervallo predefinito della factory.

Nota: per il parametro deindex, è necessario specificare un argomento factory.

Esempio di parametri di sincronizzazione

```
pdm_k_reindex sync[:purge|restore] factory:KD|cr|jss|all
```

Nota: se si omette la modalità di eliminazione o ripristino, vengono richiamate entrambe le modalità. Inoltre, per il parametro sync, è necessario specificare un argomento factory.

Parametri vari

```
pdm_k_reindex -pm
```

Corregge i collegamenti del documento e le immagini incorporate all'interno del campo della risoluzione.

```
pdm_k_reindex -ml
```

Corregge i collegamenti del documento all'interno del campo della risoluzione e li mappa al database.

Nota: per ulteriori informazioni sull'utilità pdm_k_reindex, consultare la *Guida all'implementazione*.

Aumento delle capacità di ricerca

Se si installa il motore del modulo di ricerca FAST ESP in CA Service Desk Manager per migliorare le ricerche della conoscenza, il contratto di licenza predefinito per il motore di ricerca specifica le seguenti limitazioni:

- Due ricerche al secondo
- Due milioni di oggetti indicizzati

Se si ha necessità di aumentare le funzionalità di ricerca specificate dall'accordo di licenza, rivolgersi a FAST e acquistare licenze aggiuntive all'indirizzo CAKnowledgeT@fastsearch.com.

Modalità di esecuzione del backup dei dati di FAST ESP

Dopo aver installato, configurato e utilizzato il motore di ricerca FAST ESP, è necessario effettuare regolarmente varie operazioni di manutenzione per garantire il corretto backup dei dati di FAST ESP. La frequenza con cui eseguire il backup dei dati dipende dalle esigenze aziendali. Se la configurazione cambia continuamente o se viene regolarmente aggiunto nuovo contenuto, è consigliabile eseguire il backup con maggiore frequenza.

Per eseguire il backup dei dati di FAST ESP, completare la procedura seguente:

1. Eseguire il backup delle directory seguenti:
 - \$FASTSEARCH/data/data_fixml
 - \$FASTSEARCH/data/data_index
 - FASTSEARCH/etc
2. Eseguire il backup dei profili di indice nel percorso seguente:
 - FASTSEARCH/index-profiles

Nota: per informazioni complete su backup e ripristino dei dati di FAST ESP, consultare il documento *FAST ESP Operations Guide*.

Integrazione di FAST ESP nel server secondario

È possibile utilizzare il prodotto per integrare FAST ESP nel server secondario.

Per integrare FAST ESP nel server secondario

1. Fare clic sulla scheda Amministrazione.
Viene visualizzata la console di amministrazione.
2. Nella struttura a sinistra, fare clic su Gestione opzioni, Motore di ricerca.
Viene visualizzato l'Elenco opzioni.
3. Specificare l'impostazione seguente nel server secondario:

ebr_version

Specificare FAST [Motore di ricerca].

ebr_search_engine_baseport

Specificare la porta di base del server dedicato nel quale è installato il motore del modulo di ricerca FAST ESP. Prendere in considerazione quanto segue quando si specifica la porta di base:

- Assicurarsi che il numero di porta immesso qui corrisponda alla porta di base specificata durante l'installazione di FAST ESP (la porta predefinita è 13000).
- La porta di base viene utilizzata da FAST ESP per calcolare le porte statiche.

- In ciascun host è necessario che sia presente una serie di 4000 porte tra la porta di base FAST ESP e l'installazione FAST ESP perché FAST ESP sposta le porte statiche dalla porta di base (ovvero, il numero di porta dell'interfaccia di amministrazione se è 16000).
- Assicurarsi che questo intervallo di porte non confligga con altri prodotti o servizi utilizzati dal server.
- Non è possibile utilizzare porte sotto la 1024.
- È consigliato di *non* usare una porta di base nella serie da 23000 a 27000, poiché il server delle licenze utilizza sempre il numero di porta 27000.

Importante tutti gli host devono possedere l'accesso illimitato alla rete per l'intero intervallo di porte (ad esempio, le porte da 13000 a 16999).

ebr_search_engine_host

Specificare il nome di dominio qualificato o l'indirizzo IP (consigliato) del server dedicato sul quale è installato il motore del modulo di ricerca FAST ESP.

4. Fare clic su Salva, Aggiorna.
La pagina dei dettagli delle opzioni viene aggiornata con la propria selezione.
5. Fare clic su Chiudi finestra.
6. Fermare e avviare il servizio denominato server CA Service Desk Manager.

Modalità di configurazione di CA Workflow

Per configurare CA Workflow per l'utilizzo con l'installazione di CA Service Desk Manager, eseguire le attività descritte in questa sezione.

Ulteriori informazioni:

[Avvio e arresto di CA Workflow](#) (a pagina 211)

[Impostazione dell'accesso automatico \(autenticazione esterna\)](#) (a pagina 214)

[Configurazione di Gestione elenco di lavoro e Gestione flusso di lavoro per l'accesso automatico.](#) (a pagina 216)

[Configurazione di Workflow Design Environment per l'accesso automatico](#) (a pagina 217)

[Opzioni del flusso di lavoro CA](#) (a pagina 218)

[Modalità di configurazione del flusso di lavoro di esempio per Gestione dei problemi](#) (a pagina 219)

[Modalità di configurazione del flusso di lavoro di esempio per Ordine computer](#) (a pagina 221)

[Esempio di modifica delle definizioni del processo di gestione](#) (a pagina 222)

Avvio e arresto di CA Workflow

Prima di installare CA Workflow è necessario installare e configurare CA Service Desk Manager. L'istanza Tomcat predefinita di CA Service Desk Manager viene configurata, avviata e arrestata automaticamente dalla Gestione daemon CA Service Desk Manager. Per avviare e arrestare l'istanza Tomcat, è possibile anche utilizzare l'utilità della riga di comando `pdm_tomcat_nxd`.

Per avviare e arrestare CA Workflow

1. Installare e configurare il server CA Service Desk Manager primario.
2. Installare e configurare il server CA Service Desk Manager secondario, se si intende installare CA Workflow in un server secondario.
3. Eseguire `pdm_edit` (nel server primario) per configurare processi specifici da avviare nel server secondario.
4. Riavviare i servizi CA Service Desk Manager.

Verrà effettuato il controllo della versione di variabili di ambiente specifiche in un server secondario necessarie per l'installazione e l'esecuzione di CA Workflow.

5. Installare e configurare CA Workflow.
6. Eseguire il comando `pdm_tomcat_nxd -d start -t CAWF`

CA Workflow verrà avviato manualmente.

Nota: per arrestare CA Workflow, eseguire il comando `pdm_tomcat_nxd -d stop -t CAWF`.

7. Installare le opzioni di CAWF nel server primario.

Questa operazione consente l'avvio e l'arresto automatico di CA Workflow e consentirà le comunicazioni tra CA Service Desk Manager e CA Workflow.

Ulteriori informazioni:

[pdm_tomcat_nxd: avvio o arresto di un'istanza di Tomcat](#) (a pagina 212)

pdm_tomcat_nxd: avvio o arresto di un'istanza di Tomcat

L'utilità *pdm_tomcat_nxd* viene eseguita come processo daemon e come utilità della riga di comando. L'utilità può eseguire le operazioni seguenti:

- Gestisce le richieste provenienti dall'utilità della riga di comando di avviare e arrestare una specifica istanza di Tomcat
- Restituisce lo stato di Tomcat.
- Chiude il daemon e arresta l'istanza di Tomcat.

Il daemon gestisce, inoltre, le richieste da un servlet listener Tomcat per aggiornare lo stato dell'istanza Tomcat quando viene arrestata o avviata.

L'utilità della riga di comando *pdm_tomcat_nxd* indirizza le richieste START, STOP, STATUS ed EXIT ad un daemon Tomcat. In alternativa, può avviare o arrestare una specifica istanza di Tomcat direttamente, senza utilizzare un daemon Tomcat.

Pdm_tomcat_nxd rende disponibili più daemon, che vengono avviati su un singolo server CA Service Desk Manager, ciascuno dei quali gestisce una specifica istanza di Tomcat. Ogni daemon viene inizializzato con un nome Tomcat e Server specifico, utilizzato per comporre l'indirizzo slump del daemon, l'indirizzo slump del listener e la directory di base di Catalina in cui è definita l'istanza Tomcat. Questo cambiamento è supportato da un nuovo parametro per i nomi Tomcat.

Utilizzare il comando seguente per avviare un daemon *pdm_tomcat_nxd*. Quando il daemon viene avviato, avvia automaticamente un'istanza di Tomcat con un nome Tomcat specificato.

Nota: negli esempi seguenti il nome Tomcat predefinito è vuoto (ovvero "ServiceDesk").

```
pdm_tomcat_nxd -s [-t tomcat]
```

Esempio: inviare una richiesta ad un daemon Tomcat specifico su un server specifico

Se la richiesta è STATUS, viene prima inviato un messaggio al listener Tomcat. Se non si riceve risposta, la richiesta viene inviata al daemon Tomcat. Il nome server predefinito è NX_LOCAL_HOST. Il nome Tomcat predefinito è vuoto (ovvero "ServiceDesk").

```
pdm_tomcat_nxd -c <richiesta> [-t <nome_tomcat>] [-S <nome_server>]
```

richiesta

STOP | SHUTDOWN | START | STATUS | EXIT

Esempio: avviare o arrestare un Tomcat specifico su questo server (senza utilizzare il daemon Tomcat)

```
pdm_tomcat_nxd -d <richiesta> [-t <nome_tomcat>]
```

richiesta

STOP | START

Esempio: visualizzare il comando Tomcat che verrà utilizzato per avviare e arrestare un'istanza di Tomcat

```
pdm_tomcat_nxd -T [-t <nome_tomcat>]
```

Quando il processo daemon viene avviato, accede al server slump utilizzando un nome di processo composto dal nome server e dal nome tomcat (se non è vuoto). L'utilità della riga di comando utilizza questo indirizzo per inviare messaggi al daemon. Per inviare le richieste STATUS al listener Tomcat, l'utilità della riga di comando utilizza il nome processo del listener, anch'esso composto dal nome server e dal nome Tomcat (se non è vuoto). Il daemon inoltre apre un file di registro per l'istanza di Tomcat utilizzando un nome file di registro composto dal nome tomcat (se non è vuoto). Nell'esempio seguente vengono visualizzate le variabili del nome daemon, del nome listener e del nome file di registro:

```
nome_daemon
```

```
"pdm_tomcat -" +  
nome_server:  
[ + "-" + nome_tomcat ] se nome_tomcat non è vuoto
```

```
nome_listener = nome_server + "-" +  
"container-pdmContextListener"  
[ + "-" + nome_tomcat ] se nome_tomcat non è vuoto
```

```
registro_tomcat = pdm_tomcat +  
[ + "-" + nome_tomcat ] se nome_tomcat non è vuoto  
.log
```

Quando l'utilità della riga di comando o il processo daemon avvia o arresta un'istanza Tomcat, viene generato un comando (`catalina_cmd`) con diverse variabili di ambiente NX. Tutte le variabili di ambiente che seguono sono necessarie, ad eccezione di `NX_JAVA_OPTIONS` e `NX_TOMCAT_HOTSPOT`, utilizzate solo nei sistemi HP.

I nomi delle variabili di ambiente (per l'istanza Tomcat ServiceDesk predefinita) non includono un nome Tomcat. Per i nomi delle variabili di ambiente per tutte le altre istanze Tomcat si può scegliere di utilizzare un nome Tomcat, ad eccezione di NX_XXX_CATALINA_BASE, in cui il nome tomcat (XXX) deve essere necessariamente specificato. Se non esiste una variabile di ambiente specifica di Tomcat, viene utilizzato il nome della variabile di ambiente predefinito.

```
CATALINA_BASE | NX_XXX_CATALINA_BASE
NX_TOMCAT_INSTALL_DIR + [_XXX]
NX_TOMCAT_INSTALL_DIR + [_XXX]
NX_JRE_INSTALL_DIR + [_XXX]
NX_JDBC_DRIVER + [_XXX]
NX_JAVA_OPTIONS + [_XXX]
NX_JDBC_DRIVER_CLASSPATH + [_XXX]
NX_TOMCAT_HOTSPOT + [_XXX]
```

Impostazione dell'accesso automatico (autenticazione esterna)

Per autenticare il processo di accesso delle attività dell'elenco lavori CA Workflow quando si opera con ordini di cambiamento, richieste, incidenti, problemi e questioni, è possibile impostare l'accesso automatico. Quando si utilizza l'accesso automatico, non sarà necessario immettere un ID utente e una password quando si fa clic sul collegamento Elenco lavori. L'accesso automatico utilizza le credenziali di dominio del proprio sistema operativo Windows per effettuare l'accesso all'Elenco lavori.

Nota: perché l'accesso automatico funzioni in modo corretto, l'utente *non* deve essere incluso nei gruppi Amministratori del flusso di lavoro, Iniziatori del processo del flusso di lavoro o Workflow SuperUser in CA EEM. Questi gruppo offrono diversi livelli di accesso ad utenti che hanno effettuato l'accesso a Workflow Design Environment.

Per impostare l'accesso automatico per attività di elenco lavori (solo Windows)

1. [Installazione e configurazione di CA Workflow](#). (a pagina 142)
2. [Configurare Gestione elenco di lavoro e Gestione flusso di lavoro in modo che utilizzino l'accesso automatico](#) (a pagina 216).
3. Configurare CA EEM in modo che faccia riferimento ad una directory esterna (ad esempio, Microsoft Active Directory) per l'autenticazione degli utenti. Per informazioni, vedere la propria documentazione CA EEM.

Nota: per accedere ad Elenco lavori e per il corretto funzionamento di Accesso automatico, è necessario che un utente disponga di un record utente CA EEM, nonché di un record di contatto CA Service Desk Manager corrispondente valido per lo stesso account utente. Per consentire la visualizzazione di un elemento in Elenco lavori e per sfruttare i gruppi Amministratori del flusso di lavoro, Iniziatori del processo del flusso di lavoro e Workflow SuperUser in CA EEM, è necessario un record utente CA EEM valido.

4. Accedere a CA Service Desk Manager.
5. Fare clic sulla scheda Amministrazione.
6. Nella struttura a sinistra, fare clic su Gestione opzioni, CA Workflow.
Viene visualizzato l'Elenco opzioni.
7. Verificare che il nome utente in `cawf_username` e la password in `cawf_password` corrispondano ad un utente valido nella configurazione di dominio in CA EEM. In caso contrario, utilizzare CA EEM per aggiungere l'utente al dominio.

Importante in Gestione opzioni, i valori in `cawf_username` e `cawf_password` sono impostati in base ai valori specificati per nome utente con privilegi e password dell'utente con privilegi quando si configura CA Service Desk Manager dopo l'installazione. Se l'utente con privilegi specificato durante la configurazione di CA Service Desk Manager non è disponibile quando CA EEM viene configurato in modo da fare riferimento alla directory esterna, *non* sarà possibile effettuare l'accesso automatico. In questa situazione utilizzare CA EEM per aggiungere l'utente al dominio oppure cambiare le informazioni in `cawf_username` e `cawf_password` includendo una configurazione di dominio valida in CA EEM.

8. Effettuare l'accesso a CA Service Desk Manager e creare un ordine di cambiamento, una richiesta, un incidente, un problema o una questione con la categoria appropriata.

Nota: assicurarsi che la categoria sia configurata per l'uso di CA Workflow e disponga di una definizione CA Workflow collegata prima di creare l'ordine di cambiamento, la richiesta, l'incidente, il problema o la questione.

Ora sarà possibile fare clic su un collegamento nell'Elenco lavori ed effettuare l'accesso senza ricevere la richiesta di ID utente e password.

Ulteriori informazioni:

[Configurazione di Workflow Design Environment per l'accesso automatico](#) (a pagina 217)

Configurazione di Gestione elenco di lavoro e Gestione flusso di lavoro per l'accesso automatico.

Per attivare l'accesso automatico per Gestione elenco di lavoro e Gestione flusso di lavoro, modificare il valore della variabile *automaticLoginEnabled* su true nei rispettivi file web.xml (wl.xml e pm.xml). Le voci sono le stesse in entrambi i file web.xml.

```
<env-entry>
  <env-entry-name>automaticLoginEnabled</env-entry-name>
  <env-entry-value>true</env-entry-value>
  <env-entry-type>java.lang.Boolean</env-entry-type>
</env-entry>
```

Il valore iniziale per Gestione elenco di lavoro e Gestione flusso di lavoro è definito durante l'installazione in base all'impostazione nel file di risposta.

Abilitare o disabilitare Accesso automatico (noto anche come Single Sign On o SSO)

-P serverAction.automaticLoginEnabled="true"

Per configurare Gestione elenco di lavoro e Gestione flusso di lavoro per l'accesso automatico.

1. Accedere ai file pm.xml e wl.xml nella directory seguente:
\$NX_ROOT\bopcfg\www\CATALINA_BASE_WF\conf\Catalina\localhost
2. Modificare pm.xml e wl.xml e cambiare il valore della riga seguente:
 - (Prima della modifica) <Nome ambiente="automaticLoginEnabled" override="true" type="java.lang.Boolean" value="false"/>
 - (Dopo la modifica) <Nome ambiente="automaticLoginEnabled" override="true" type="java.lang.Boolean" value="true"/>
3. Arrestare il server Tomcat utilizzando il comando seguente:
pdm_tomcat_nxd -d STOP -t CAWF
4. Avviare il server Tomcat per ricreare queste due cartelle utilizzando il comando seguente:
pdm_tomcat_nxd -d START -t CAWF
5. Accedere ad un ticket con un'attività del flusso di lavoro e selezionare una delle attività.
6. Viene visualizzato Elenco lavori e l'accesso viene eseguito correttamente.

Nota: se si riconfigura CA Workflow e si fa riferimento ad un server CA EEM diverso, è necessario arrestare CAWF Tomcat, eliminare entrambe le cartelle *pm* e *wl* in \$NX_ROOT\bopcfg\www\CATALINA_BASE_WF\webapps, quindi riavviare CAWF Tomcat per ricreare nuovamente le cartelle con le nuove informazioni del server CA EEM.

Configurazione di Workflow Design Environment per l'accesso automatico

L'accesso automatico per Workflow Design Environment viene abilitato mediante il parametro della riga di comando *-auto*.

Opzioni del flusso di lavoro CA

La funzione CA Workflow è controllata dalle opzioni indicate di seguito.

Importante Dopo aver installato CA Workflow e CA EEM, inserire manualmente opzioni quali il numero di porta in Gestione opzioni. Ad esempio, l'impiego di un'applicazione Web Tomcat separata per CA Workflow non consente di utilizzare la porta predefinita 8080. Per evitare il conflitto delle porte, si utilizza il valore predefinito 8090. Per ulteriori informazioni, consultare la *Guida all'implementazione*.

cawf_hostname

Consente di specificare il nome host del server nel quale è installato CA Workflow. Impostare questa variabile solo se CA Workflow è installato dai supporti CA Service Desk Manager; in caso contrario, non installarla.

cawf_password

Consente di specificare la password per l'utente CA Workflow IDE. Durante l'installazione di CA Workflow, la procedura guidata di installazione dei componenti di CA Service Desk Manager utilizza il valore Password utente flusso di lavoro per impostare cawf_password.

cawf_pm_location

Consente di specificare la posizione dell'applicazione Gestione processi CA Workflow. L'URL deve presentare il seguente formato:

`http://<wf_hostname>:8090/pm`

cawf_pm_url

Consente di specificare l'URL del servizio Web dell'applicazione Gestione processi CA Workflow. L'URL deve presentare il seguente formato:

`http://<wf_hostname>:8090/pm/services/pmService2`

cawf_username

Consente di specificare il nome utente CA Workflow per l'utente CA Workflow IDE. Durante l'installazione di CA Workflow, la procedura guidata di installazione dei componenti di CA Service Desk Manager utilizza il valore Nome utente flusso di lavoro per impostare cawf_username.

cawf_wl_location

Consente di specificare la posizione dell'applicazione Elenco di lavoro CA Workflow. L'URL deve presentare il seguente formato:

`http://<wf_hostname>:8090/wl`

cawf_wl_url

Consente di specificare l'URL del servizio Web dell'applicazione Elenco di lavoro CA Workflow. L'URL deve presentare il seguente formato:

`http://<wf_hostname>:8090/wl/services/wlService`

Nota: l'installazione di queste opzioni richiede il riavvio del server CA Service Desk Manager.

Modalità di configurazione del flusso di lavoro di esempio per Gestione dei problemi

Il flusso di lavoro di esempio Gestione dei problemi determina il processo per decidere se creare un ordine di cambiamento per un ticket di problema particolare. Dopo che un assegnatario problema ha effettuato la ricerca di un problema, completa l'indagine per sviluppare un consiglio. L'indagine dà al revisore un'idea circa l'impatto del problema e indica se è necessario risolverlo attraverso la gestione dei cambiamenti. Il concetto sottostante di questo flusso di lavoro (sintomo del problema/analisi valore) viene derivato da ITIL v3.

Nota: per i dettagli relativi all'esecuzione delle attività CA Service Desk Manager nei processi seguenti, vedere la *Guida in linea*.

Per configurare il flusso di lavoro di esempio per Gestione dei problemi

1. Creare un contatto CA Service Desk Manager per un analista (ad esempio, Analista Jane) utilizzando i valori seguenti:

Tipo contatto

Selezionare Analista.

Partizione dati

Selezionare Analista Service Desk.

Tipo di accesso

Selezionare Staff Service Desk.

Indirizzo di posta elettronica

Immettere un indirizzo di posta elettronica.

Nota: per motivi di testing, è possibile immettere il proprio indirizzo di posta elettronica.

Metodo di notifica

Selezionare Posta elettronica per le notifiche Basso, Normale, Alto e Emergenza.

2. Creare un contatto CA Service Desk Manager per un supervisore (ad esempio, Supervisore Joe) utilizzando i valori seguenti:

Tipo contatto

Selezionare Manager.

Partizione dati

Selezionare Amministratore Service Desk.

Tipo di accesso

Selezionare Gestione Service Desk.

Indirizzo di posta elettronica

Immettere un indirizzo di posta elettronica.

Nota: per motivi di testing, è possibile immettere il proprio indirizzo di posta elettronica.

Metodo di notifica

Selezionare Notifica per le notifiche di livello Basso, Normale, Alto ed Emergenza.

3. Creare un record utente EEM associato per i contatti CA Service Desk Manager Analista Jane e Supervisore Joe.
Nota: gli ID utente dei record EEM devono corrispondere a quelli dei record di contatto. Per informazioni sulla creazione di record utente EEM, vedere la *Guida in linea di EEM*.
4. Assegnare a Supervisore Joe il ruolo di supervisore del record del contatto Analista Jane.
5. Creare un elemento della configurazione (ad esempio, Exchange Server).
6. Creare un codice di causa principale (ad esempio, Aggiornamento RAM necessario).
7. Creare un'area problema (ad esempio ProblemMgmt.SampleWF).
8. Associare l'area problema ProblemMgmt.SampleWF al flusso di lavoro di esempio Gestione problema.
9. Creare un ticket di problema con gli attributi seguenti:

Area problema

Selezionare ProblemMgmt.SampleWF.

Elemento di configurazione

Selezionare Exchange Server.

Assegnatario

Selezionare Analista, Jane.

10. Effettuare l'accesso a CA Service Desk Manager come Analista Jane e testare la configurazione del flusso di lavoro.
Nota: prima di poter completare il primo modulo del flusso di lavoro, è necessario completare la ricerca del problema. Per informazioni sull'esecuzione delle attività del flusso di lavoro, vedere la *Guida in linea di CA Workflow*.

Ulteriori informazioni:

[Impostazione dell'accesso automatico \(autenticazione CA MDB\)](#) (a pagina 233)

[Impostazione dell'accesso automatico \(autenticazione esterna\)](#) (a pagina 214)

[Avvio e arresto di CA Workflow](#) (a pagina 211)

Modalità di configurazione del flusso di lavoro di esempio per Ordine computer

Il flusso di lavoro di esempio Ordine computer determina il processo di gestione dei cambiamenti se occorre ordinare un nuovo computer.

Nota: per i dettagli relativi all'esecuzione delle attività CA Service Desk Manager nei processi seguenti, vedere la *Guida in linea*.

Per configurare e verificare il flusso di lavoro di esempio Ordine computer:

1. Creare un contatto CA Service Desk Manager per un dipendente (ad esempio, Dipendente William) utilizzando i valori seguenti:

Tipo contatto

Selezionare Dipendente.

Partizione dati

Selezionare Dipendente.

Tipo di accesso

Selezionare Dipendente.

Indirizzo di posta elettronica

Immettere un indirizzo di posta elettronica.

Nota: per motivi di testing, è possibile immettere il proprio indirizzo di posta elettronica.

Metodo di notifica

Selezionare Posta elettronica per le notifiche Basso, Normale, Alto e Emergenza.

2. Creazione di un contatto CA Service Desk Manager per un analista (ad esempio, Analista Jane) utilizzando i valori seguenti:

Tipo contatto

Selezionare Analista.

Partizione dati

Selezionare Analista Service Desk.

Tipo di accesso

Selezionare Staff Service Desk.

Indirizzo di posta elettronica

Immettere un indirizzo di posta elettronica.

Nota: per motivi di testing, è possibile immettere il proprio indirizzo di posta elettronica.

Metodo di notifica

Selezionare Posta elettronica per le notifiche Basso, Normale, Alto e Emergenza.

3. Creare un record utente EEM associato per i contatti CA Service Desk Manager Analista Jane e Dipendente William.

Nota: gli ID utente dei record EEM devono corrispondere a quelli dei record di contatto. Per informazioni sulla creazione di record utente EEM, vedere la *Guida in linea di EEM*.

4. Creare una categoria di cambiamento (ad esempio PC.Order).
5. Definire Giovanna Analista come assegnatario della categoria di cambiamento.
6. Creare un ticket di ordine di cambiamento con i seguenti attributi:

Categoria modifica

Selezionare PC.Order.

Assegnatario

Selezionare Analista, Jane.

7. Effettuare l'accesso a CA Service Desk Manager come Analista Jane e testare la configurazione del flusso di lavoro.

Nota: per informazioni sull'esecuzione delle attività del flusso di lavoro, vedere la *Guida in linea di CA Workflow*.

Esempio di modifica delle definizioni del processo di gestione

In questo esempio viene dimostrato in che modo la definizione del processo di gestione dei cambiamenti gestisce gli ordini di cambiamento in base alle linee guida ITIL v3 seguenti:

- Valutazione dei rischi
- Analisi conflitto e impatto

- Approvazione Gestione cambiamento e CAB
- Valutazione e analisi dell'implementazione

Nota: in questo esempio si suppone che CA Service Desk Manager utilizzi CA Workflow e che la definizione del processo di gestione dei cambiamenti sia impostata. Per informazioni sull'impostazione della definizione del processo di gestione dei cambiamenti, consultare la *Guida all'amministrazione*.

Modalità di preparazione di un ordine di cambiamento per l'approvazione

In questo esempio viene configurata una categoria di cambiamento e preparato un ordine di cambiamento per l'approvazione. L'amministratore configura la categoria di cambiamento per l'utilizzo della definizione del processo di gestione dei cambiamenti e l'impostazione di gruppi e contatti. Il richiedente completa un'indagine per la valutazione dei rischi, esegue l'analisi dei conflitti e dell'impatto e l'analisi del cambiamento.

Nota: per informazioni sulla configurazione della categoria di cambiamento e sull'utilizzo della definizione del processo di gestione dei cambiamenti, vedere la *Guida in linea* e la *Guida all'amministrazione*.

Per preparare un ordine di cambiamento per l'approvazione, effettuare le operazioni seguenti:

1. Accedere come amministratore, creare o modificare una categoria di cambiamento con le opzioni riportate di seguito e fare clic su Usa CA Workflow:
 - **CAB**—Selezionare il gruppo CAB.
 - **Gruppo**—Specificare il gruppo Implementazione.
 - **Indagine rischio**—Selezionare Generale.
 - **Nome definizione CA Workflow**—Selezionare Change Mgmt (Gestione cambiamenti) - Service Desk r12.1 (nella scheda Flusso di lavoro).
2. Creare i contatti e gli ID utente CA Service Desk Manager seguenti e assegnarli ai rispettivi gruppi in CA Service Desk Manager e CA EEM:
 - **Richiedente Don**—Contatto che crea l'ordine di cambiamento.
 - **Approvatore John**—Responsabile del gruppo Implementazione con funzioni di Gestione cambiamento per l'approvazione di un ordine di cambiamento. Responsabile del gruppo CAB che agisce da approvatore CAB.

- **Implementatore Sue**—Membro del gruppo Implementazione che completa anche gli elementi di lavoro degli ordini di cambiamento.
3. Accedere come Richiedente Don e creare un ordine di cambiamento con i valori seguenti:
- **Richiedente**—Specificare Richiedente Don.
 - **Categoria**—Specificare la categoria di cambiamento con la definizione del processo di gestione dei cambiamenti.
 - **Tipo**—Selezionare Normale.
 - **Riepilogo Ordine/Descrizione Ordine**—Specificare il motivo dell'ordine di cambiamento.
 - **Data di inizio pianificazione**—Specificare una data iniziale.
 - **Durata pianificazione**—Specificare la durata.
 - **Elementi della configurazione**—Specificare gli elementi della configurazione interessati (nella scheda Elementi della configurazione).

Richiedente Don riceve una notifica tramite posta elettronica per il completamento dell'indagine per la valutazione dei rischi. Nella pagina Dettagli ordine di cambiamento viene mostrato lo stato RFC.

4. Fare clic su Indagine di rischio e rispondere alle domande dell'indagine per la valutazione dei rischi in modo che l'ordine di cambiamento presenti un Rischio elevato. Fare clic su Inoltra e Conferma.

Viene generato un valore di rischio per l'ordine di cambiamento e il richiedente riceve una notifica tramite posta elettronica per l'avvio dell'analisi dei conflitti e dell'impatto.

Nota: dopo aver selezionato Conferma nella pagina Esegui attività è possibile passare solo all'attività successiva.

5. Nella scheda Attività flusso di lavoro seguire i collegamenti per passare alla scheda Conflitti dell'ordine di cambiamento.
6. Fare clic su Analisi conflitto per esaminare e risolvere tutte i conflitti di pianificazione per gli elementi della configurazione.
7. Nella scheda Elementi della configurazione fare clic su Analisi impatto per esaminare le informazioni su ogni elemento della configurazione.
8. Nella scheda Elementi della configurazione fare clic su Impact Explorer e passare alla scheda Relazioni CMDB per considerare l'impatto dell'ordine di cambiamento sugli elementi della configurazione correlati.

9. Passare alla pagina Esegui attività e fare clic su Conferma.

Richiedente Don riceve una notifica tramite posta elettronica per l'esecuzione dell'analisi del cambiamento.

10. Nella scheda Attività flusso di lavoro seguire i collegamenti per passare alla scheda Analisi cambiamento+++. Rispondere alle domande per confermare l'ordine di cambiamento e fare clic su Inoltra.

Approvatore John riceve una notifica tramite posta elettronica per l'approvazione dell'ordine di cambiamento. Nella pagina Dettagli ordine di cambiamento viene mostrato quanto segue:

- Stato-Approvazione in corso
- Approvazione CAB-Sì

Modalità di approvazione e implementazione dell'ordine di cambiamento

In questo esempio vengono illustrate le attività di approvazione e implementazione da eseguire durante l'utilizzo della definizione del processo di gestione dei cambiamenti per gestire gli ordini di cambiamento.

L'approvatore esamina le informazioni dell'analisi del cambiamento e approva l'ordine di cambiamento. Un membro del gruppo di implementazione completa il lavoro assegnato sull'ordine di cambiamento e un'analisi post-implementazione che descrive il risultato dell'ordine di cambiamento.

Nota: per informazioni sull'utilizzo della definizione del processo di gestione dei cambiamenti, consultare la *Guida all'amministrazione*.

Per approvare e implementare l'ordine di cambiamento, effettuare le operazioni seguenti:

1. Accedere come Approvatore John e aprire l'ordine di cambiamento.
2. Nella scheda Attività flusso di lavoro seguire i collegamenti per passare alla scheda Chg Mgr Approval+++ e fare clic su Approva.

L'ordine di cambiamento presenta un Rischio elevato e pertanto lo stato sarà Approvazione in corso. Poiché in questo esempio Approvatore John viene utilizzato anche come membro del comitato CAB, riceverà una notifica tramite posta elettronica per l'analisi dell'ordine di cambiamento in qualità di membro CAB.

3. Nella scheda Approvazione CAB fare clic su Approva.

Nella pagina Dettagli ordine di cambiamento viene mostrato lo stato Approvato. Implementatore Sue riceve una notifica tramite posta elettronica.

4. Accedere come Implementatore Sue e aprire l'ordine di cambiamento.

5. Nella scheda Attività flusso di lavoro passare alla pagina Esegui attività e fare clic su Conferma.

Nella pagina Dettagli ordine di cambiamento viene mostrato lo stato Implementazione in corso.

6. Nella scheda Attività flusso di lavoro seguire i collegamenti per passare alla scheda di completamento dell'implementazione.

7. Rispondere alle domande per descrivere lo stato di avanzamento dell'ordine di cambiamento e fare clic su Completato.

L'ordine di cambiamento viene chiuso. Nella pagina Dettagli ordine di cambiamento viene mostrato lo stato Implementato e il codice di chiusura Riuscito. Implementatore Sue riceve una notifica tramite posta elettronica per l'esecuzione della revisione post-implementazione (PIR).

8. Nella scheda Attività flusso di lavoro seguire i collegamenti per passare alla scheda PIR.

9. Nella scheda PIR rispondere alle domande per descrivere la risoluzione e fare clic su Inoltra.

L'ordine di cambiamento viene chiuso. Nella pagina Dettagli ordine di cambiamento viene mostrato lo stato Chiuso. Nella scheda Attività flusso di lavoro viene mostrato il collegamento Chiudi Ordine di cambiamento con informazioni aggiuntive. Nella scheda Attività Ordine di cambiamento viene mostrato lo stato finale della definizione del processo di gestione dei cambiamenti.

Modalità di configurazione dell'integrazione del flusso di lavoro di CA IT PAM

Per configurare l'integrazione del flusso di lavoro di CA IT PAM, effettuare le operazioni seguenti:

1. Verificare che CA IT PAM e CA Service Desk Manager funzionino come entità autonome.
2. Configurare le opzioni del flusso di lavoro di CA IT PAM.
3. Creare i gruppi e gli ID utente necessari per concedere agli utenti di CA Service Desk Manager l'accesso appropriato a CA IT PAM.

Ulteriori informazioni:

[Verificare le installazioni di CA IT PAM e CA Service Desk Manager](#) (a pagina 227)

[Configurazione delle opzioni del flusso di lavoro di CA IT PAM](#) (a pagina 227)

[Amministrazione utente CA IT PAM](#) (a pagina 230)

[Modalità di supporto del Single Sign-On da CA Service Desk Manager a CA IT PAM mediante CA EEM](#) (a pagina 232)

Verificare le installazioni di CA IT PAM e CA Service Desk Manager

È possibile integrare CA IT PAM e CA Service Desk Manager in modo che coesistano su un singolo server quando l'architettura server supporta entrambi i prodotti. Se i componenti CA IT PAM o CA Service Desk Manager non possono essere integrati sullo stesso server, installare ogni prodotto su un server distinto.

Prima di configurare CA IT PAM e CA Service Desk Manager, è possibile verificare che entrambi i prodotti siano installati e funzionino in modo indipendente.

Nota: per informazioni sui requisiti dei prodotti CA Service Desk Manager e CA IT PAM, consultare le <Note di rilascio di CA Service Desk Manager>.

Per verificare le installazioni di CA IT PAM e CA Service Desk Manager

1. Aprire un browser sul server che ospita CA Service Desk Manager e verificare che un utente di CA IT PAM possa accedere a CA IT PAM. Modificare i segnaposto che corrispondono all'installazione di CA IT PAM di destinazione.

`http(s)://<server>:Portale CA/itpam`

2. Immettere l'URL seguente: Modificare i segnaposto in modo che corrispondano all'installazione di CA IT PAM di destinazione.

`http(s)://<server>:Portale CA/itpam/JNLPRquestProcessor?processType=startUI`

Il prodotto CA IT PAM è accessibile dall'host di CA Service Desk Manager.

Configurazione delle opzioni del flusso di lavoro di CA IT PAM

Quando si configurano le opzioni del flusso di lavoro di CA IT PAM, si specifica la connettività tra CA Service Desk Manager e CA IT PAM. Se si utilizza CA EEM per l'autenticazione, è necessario specificare anche il nome host di CA EEM.

Per configurare le opzioni del flusso di lavoro di CA IT PAM

1. Nella scheda Amministrazione selezionare Gestione opzioni, Flusso di lavoro di CA IT PAM.

Viene visualizzato l'Elenco opzioni.

2. Fare clic con il pulsante destro del mouse sul nome di ogni opzione e selezionare Modifica dal menu di scelta rapida. Configurare le opzioni seguenti:

caextwf_eem_hostname

Specifica il nome del server CA EEM. Ad esempio, *http://pam.host.com* identifica l'host di autenticazione. `caextwf_eem_hostname` va installato solo se CA IT PAM è stato configurato per l'utilizzo di CA EEM come server di autenticazione. CA Service Desk Manager utilizza questo valore per trasformare una password e un nome utente in un token CA EEM, in modo che non passino come testo normale durante la comunicazione HTTP.

Nota: se l'installazione CA IT PAM non utilizza CA EEM, non immettere un valore nell'opzione `caextwf_eem_hostname` e non installare `caextwf_eem_hostname`. Se si immette un valore errato o si installa `caextwf_eem_hostname` quando non necessario, l'integrazione non riesce.

caextwf_endpoint

Specifica l'URL che porta ai servizi Web CA IT PAM includendo la porta, il nome dell'host CA IT PAM e il percorso obbligatorio `/itpam/soap`. Ad esempio, *http://pam.host.com:Portale CA/itpam/soap* identifica il punto finale. L'installazione dell'opzione `caextwf_eem_hostname` è necessaria perché l'integrazione tra CA IT PAM e CA Service Desk Manager funzioni correttamente.

caextwf_log_categories

Specifica un elenco separato da virgole contenente nomi di categorie di registro per istanze di processo CA IT PAM da visualizzare nelle schede Richiesta, Ordine di cambiamento e Attività flusso di lavoro Questioni di CA Service Desk Manager. Ad esempio, *Operatore,Risposta,LaMiaCategoria* fornisce tre categorie di registro.

`caextwf_log_categories` si installerà in base a decisioni aziendali di competenza del personale addetto alla progettazione dei processi di CA Service Desk Manager e CA IT PAM. Questa opzione regola i dati predefiniti visualizzati nella scheda Attività flusso di lavoro per richieste, ordini di cambiamento e questioni.

Quando si installa l'opzione `caextwf_log_categories`, tutti i messaggi di registro per istanze di processo CA IT PAM della categoria Processo e delle categorie specificate vengono visualizzati nella scheda Attività flusso di lavoro. Se non si installa `caextwf_log_categories`, solo i messaggi di registro per istanze di processo CA IT PAM della categoria Processo vengono visualizzati nella scheda Attività flusso di lavoro.

Nota: per informazioni sulle categorie di messaggi di registro CA IT PAM predefinite e sulla definizione delle categorie di messaggi personalizzate, consultare la documentazione di riferimento di CA IT PAM.

caextwf_processdisplay_url

Specifica come lanciare una snapshot grafica di un'istanza di processo CA IT PAM fornendo il nome dell'host e il percorso obbligatorio `/itpam/JNLPrequestProcessor?processType=startUI&roid`. Ad esempio, *`http://pam.host.com:Portale`*
`CA/itpam/JNLPrequestProcessor?processType=startUI&roid=` avvia una snapshot di un'istanza di processo. Nella scheda Attività flusso di lavoro di una richiesta, di un ordine di cambiamento o di una questione, l'utente seleziona Visualizza processo per visualizzare la snapshot.

L'installazione dell'opzione `caextwf_processdisplay_url` è necessaria perché l'integrazione tra CA IT PAM e CA Service Desk Manager funzioni correttamente.

caextwf_worklist_url

Specifica il percorso dell'istanza di processo fornendo il nome dell'host e il percorso obbligatorio `/itpam?webPage=mytaskfilter&view=tasklist`. Ad esempio, *`http://pam.host.com:Portale`*
`CA/itpam?webPage=mytaskfilter&view=tasklist` consente agli utenti di CA Service Desk Manager di visualizzare un elenco di istanze di processi CA IT PAM che richiedono attenzione. L'elenco viene visualizzato in CA IT PAM quando l'utente di CA Service Desk Manager seleziona un collegamento associato a una qualsiasi attività elencata nella scheda Attività flusso di lavoro di una richiesta, di un ordine di cambiamento o di una questione.

L'installazione dell'opzione `caextwf_worklist_url` è necessaria perché l'integrazione tra CA IT PAM e CA Service Desk Manager funzioni correttamente.

caextwf_ws_password

Specifica la password amministrativa associata al nome utente CA IT PAM mediante l'opzione `caextwf_ws_user`. CA Service Desk Manager utilizza il nome utente e la password per accedere alle funzioni di servizio Web CA IT PAM per l'esecuzione di attività di integrazione come la selezione di moduli di richiesta di avvio, informazioni sulla definizione di processo e informazioni sulle istanze di processo.

L'installazione dell'opzione `caextwf_ws_password` è necessaria per l'integrazione tra CA IT PAM e CA Service Desk Manager. La password e il nome utente specificati richiedono il giusto accesso a CA IT PAM. Tuttavia, non è necessario che il nome utente e la password di CA IT PAM esistano nei record contatto di CA Service Desk Manager.

caextwf_ws_user

Specifica il nome utente amministrativo CA IT PAM associato al nome utente CA IT PAM dall'opzione `caextwf_ws_password`. CA Service Desk Manager utilizza il nome utente e la password per accedere alle funzioni di servizio Web di CA IT PAM per l'esecuzione di attività di integrazione come la selezione di moduli di richiesta di avvio, di informazioni sulla definizione di processo e di informazioni sulle istanze di processo o l'avvio di istanze di processo.

L'installazione dell'opzione `caextwf_ws_user` è necessaria perché l'integrazione tra CA IT PAM e CA Service Desk Manager funzioni correttamente. Il nome utente e la password specificati richiedono il giusto accesso a CA IT PAM. Tuttavia, non è necessario che il nome utente e la password di CA IT PAM esistano nei record contatto di CA Service Desk Manager.

3. Fare clic su Installa.
4. Riavviare il servizio CA Service Desk Manager.

I prodotti CA Service Desk Manager e CA IT PAM possono comunicare anche in assenza di dati di istanze di processo. CA Service Desk Manager e CA IT PAM consentono di creare definizioni di processi CA IT PAM e moduli di richieste di avvio CA IT PAM.

Nota: per ulteriori informazioni sulla creazione di definizioni di processo CA IT PAM e di moduli di richiesta di avvio CA IT PAM, consultare la *Guida all'amministrazione* e la documentazione utente di CA IT PAM.

Amministrazione utente CA IT PAM

Sia CA IT PAM che CA Service Desk Manager, come prodotti autonomi, presentano singoli requisiti per l'autenticazione e l'autorizzazione. Per supportare una strategia SOA (Service Oriented Architecture) unificata, è possibile configurare entrambi i prodotti per l'utilizzo di CA EEM per l'autenticazione.

Quando si installa CA IT PAM con CA EEM come server di autenticazione, per impostazione predefinita il programma di installazione crea diversi criteri e quattro entità fondamentali:

- Due utenti applicazione: `itpamadmin`, `itpamuser`
- Due gruppi di applicazioni: `ITPAMAdmins`, `ITPAMUsers`

Gli utenti di CA Service Desk Manager che utilizzano anche CA IT PAM possono essere divisi tra ITPAMAdmins e ITPAMUsers nel modo seguente:

- Gli analisti CA Service Desk Manager devono essere membri di ITPAMUsers quando i loro compiti comportano:
 - Approvazione, rifiuto o risposta a moduli di richiesta di interazione con CA IT PAM.
 - Creazione di elenchi di istanze di processi CA IT PAM assegnate all'utente.
 - Visualizzazione grafica mediante clic sul pulsante Visualizza processo della schermata di stato del processo CA IT PAM. Il gruppo ITPAMUsers di CA IT PAM richiede un criterio CA IT PAM aggiuntivo per concedere l'accesso alla grafica.
- Gli analisti CA Service Desk Manager sono membri di ITPAMUsers quando i loro compiti comportano:
 - Creazione e archiviazione delle definizioni di processo CA IT PAM e/o avvio dei moduli di richiesta.
 - Interruzione delle istanze di processo direttamente all'interno di CA IT PAM. Questa operazione rappresenta un'eccezione amministrativa alle procedure di integrazione previste.
 - Delega delle attività delle istanze di processo CA IT PAM.
 - Corrispondenza dell'utente con il nome utente definito in Gestione opzioni di CA Service Desk Manager.
- Gli utenti di CA Service Desk Manager non richiedono alcun accesso a CA IT PAM quando i relativi compiti comportano:
 - Creazione di richieste, ordini di cambiamento e questioni che avviano istanze di CA IT PAM.
 - Analisi della scheda Flusso di lavoro che contiene informazioni sulle attività e sullo stato delle istanze dei processi CA IT PAM.
 - Modifica dello stato di una richiesta, di un ordine di cambiamento o di una questione che genera l'interruzione di un processo CA IT PAM, ad esempio l'annullamento di un ordine di cambiamento.
 - Selezione di una definizione di processo CA IT PAM in un'area di richiesta CA Service Desk Manager, di una categoria di cambiamento e di una categoria di questione.

Nota: per informazioni sulla configurazione di CA EEM, consultare la documentazione relativa a CA IT PAM.

Modalità di supporto del Single Sign-On da CA Service Desk Manager a CA IT PAM mediante CA EEM

Quando CA Service Desk Manager e CA IT PAM sono integrati, è possibile impostare Single Sign-on per il funzionamento da CA Service Desk Manager a CA IT PAM nel modo seguente:

1. Verificare che i requisiti seguenti siano stati soddisfatti:
 - CA Service Desk Manager e CA IT PAM sono configurati per l'utilizzo della stessa installazione di CA EEM.
 - L'utente che accede a CA Service Desk Manager è anche un utente di CA IT PAM.
 - Quando CA EEM utilizza il database interno come archivio utente, gli utenti devono disporre di autorizzazioni globali o appartenere alla stessa cartella. In caso contrario, se CA EEM fa riferimento a un archivio utente esterno come una directory esterna o CA Siteminder, gli utenti devono appartenere allo stesso archivio per poter accedere a Single Sign-on.
2. Installare CA EEM dal supporto di installazione DVD di CA Service Desk Manager o utilizzare un'installazione di CA EEM esistente, ad esempio CA EEM per CA IT PAM.
3. Nella scheda Amministrazione di CA Service Desk Manager installare le opzioni seguenti da Gestione opzioni, cartella Protezione:
 - eiam_hostname
 - use_eiam_authentication

Nota: non è necessario installare l'opzione caextwf_eem_hostname in Gestione opzioni, cartella CA IT PAM. Se si esegue l'installazione, il valore deve essere identico a quello dell'opzione eiam_hostname.
4. Riavviare CA Service Desk Manager.
5. Per creare un utente in CA IT PAM, effettuare le operazioni seguenti:
 - a. Accedere a CA EEM utilizzando il contesto dell'applicazione CA IT PAM con l'ID utente EiamAdmin o qualsiasi altro utente di amministrazione.
 - b. Selezionare la scheda Gestione identità e fare clic sull'icona accanto alla cartella Utenti.

- c. Nella pagina Nuovo utente il campo Nome nella parte superiore rappresenta l'ID utente che deve corrispondere all'ID utente nella tabella contatti di CA Service Desk Manager.
 - d. Fare clic sul pulsante Aggiungi informazioni su utente applicazione ed effettuare le operazioni seguenti:
 - Aggiungere uno o entrambi i gruppi elencati. Aggiungere almeno uno di questi due gruppi in modo da accedere a CA IT PAM.
 - Completare i campi Nuovo utente, ad esempio Nome, Cognome, Visualizza e Password.
 6. Creare un utente nella tabella contatti di CA Service Desk Manager con lo stesso ID utente. Verificare che il campo relativo al tipo di validazione del tipo di accesso per l'utente sia impostato su CA EEM.
- È possibile accedere a CA EEM e CA Service Desk Manager con l'utente e la password specificati in CA EEM.

Impostazione dell'accesso automatico (autenticazione CA MDB)

Per autenticare il processo di accesso delle attività dell'elenco lavori CA Workflow quando si opera con ordini di cambiamento, richieste, incidenti, problemi e questioni, è possibile impostare l'accesso automatico. Quando si utilizza l'accesso automatico, non sarà necessario immettere un ID utente e una password quando si fa clic sul collegamento Elenco lavori. L'accesso automatico utilizza le credenziali di dominio del proprio sistema operativo Windows per effettuare l'accesso all'Elenco lavori.

Nota: perché l'accesso automatico funzioni in modo corretto, l'utente *non* deve essere incluso nei gruppi Amministratori del flusso di lavoro, Iniziatori del processo del flusso di lavoro o Workflow SuperUser in CA EEM. Questi gruppo offrono diversi livelli di accesso ad utenti che hanno effettuato l'accesso a Workflow Design Environment.

Per impostare l'accesso automatico per attività di elenco lavori (solo Windows)

1. [Installare e configurare CA Workflow.](#) (a pagina 142)
2. [Configurare Gestione elenco di lavoro e Gestione flusso di lavoro in modo che utilizzino l'accesso automatico](#) (a pagina 216).

3. Configurare CA EEM per l'uso di CA MDB per autenticare gli utenti. Quando si installa e si configura CA Workflow, vengono aggiunti automaticamente ad CA EEM il *Nome utente flusso di lavoro* e la *Password utente flusso di lavoro*. Per informazioni, vedere la propria documentazione CA EEM.

Nota: per accedere all'Elenco lavori, un utente deve disporre di un record utente CA EEM.

4. Effettuare l'accesso a CA Service Desk Manager e creare un ordine di cambiamento, una richiesta, un incidente, un problema o una questione con la categoria appropriata.

Nota: assicurarsi che la categoria sia configurata per l'uso di CA Workflow e disponga di una definizione CA Workflow collegata prima di creare l'ordine di cambiamento, la richiesta, l'incidente, il problema o la questione.

Ora sarà possibile fare clic su un collegamento nell'Elenco lavori ed effettuare l'accesso senza ricevere la richiesta di ID utente e password.

Ulteriori informazioni:

[Configurazione di Workflow Design Environment per l'accesso automatico](#) (a pagina 217)

Configurazione di punti di ingresso singoli

Quando CA Service Desk Manager e Gestione dei servizi CA sono integrati, un punto di ingresso singolo può consentire l'accesso Single Sign-on a CA Service Catalog.

Per configurare un punto di ingresso singolo

1. Installare l'opzione Generale di catalog_server.
Nota: per ulteriori informazioni, consultare la Guida in linea di Gestione opzioni.
2. Riavviare CA Service Desk Manager.
3. Passare alla pagina Self-Service dipendenti di CA Service Desk Manager.
4. Fare clic su Sfoglia servizi del catalogo.

Viene visualizzata la pagina di accesso a CA Service Management.

Se CA EEM è configurato sia per CA Service Desk Manager che per Gestione dei servizi CA, un punto di ingresso singolo può consentire l'accesso Single Sign-on a CA Service Catalog. Se Single Sign-on è configurato, la pagina di accesso a Gestione dei servizi CA non viene visualizzata.

Note: Single Sign-on non è disponibile se si accede alla pagina Self-Service dipendenti di CA Service Desk Manager come guest.

Per configurare l'accesso Single Sign-on a Gestione dei servizi CA

1. Verificare che le opzioni di protezione eiam_hostname e use_eiam_authentication di CA EEM siano installate.
2. Impostare gli utenti in CA EEM e verificare che siano anche utenti di Gestione dei servizi CA.
3. Fare clic sulla scheda Amministrazione.
4. Aprire la cartella Gestione protezione e ruoli.
5. Fare clic su Tipi di accesso.
6. Selezionare il ruolo Dipendente.
7. Verificare che il tipo di validazione nella scheda Autenticazione Web sia impostato su CA EEM-Usa CA Embedded Entitlements Manager.
8. Accedere come utente CA EEM definito e passare alla pagina Self-Service dipendenti.
9. Fare clic su Sfoglia servizi del catalogo.

Viene visualizzata la pagina principale di Gestione dei servizi CA.

Modalità di implementazione della funzione multi-tenancy

Il *fornitore del servizio* è il titolare principale di un'installazione multi-tenancy CA Service Desk Manager.

Nota: per ulteriori informazioni sul fornitore del servizio e sulla funzione multi-tenancy, consultare la *Guida all'amministrazione*.

È necessario definire i titolari e inserire l'attributo del titolare in tutti oggetti con titolare obbligatorio e con titolare facoltativo necessari prima di abilitare la funzione multi-tenancy in una modalità diversa da quella di installazione. È tuttavia possibile selezionare l'applicazione della funzione multi-tenancy prima di assegnare i titolari a tutti gli oggetti che li richiedono. Gli oggetti che non hanno un titolare in una tabella con titolare obbligatorio vengono trattati come oggetti pubblici visibili a tutti gli utenti e l'interfaccia utente rileva e supporta gli aggiornamenti per tali oggetti. A seconda dell'estensione dell'applicazione della funzione multi-tenancy, CA Service Desk Manager può richiedere o meno che un utente aggiorni un oggetto con titolare obbligatorio per fornire un titolare.

Nota: prima di poter aggiornare l'istanza di un oggetto con titolare obbligatorio, è necessario creare un titolare. È inoltre possibile utilizzare le utilità `pdm_settenant` e `pdm_buildtenant` dopo l'attivazione della funzione multi-tenancy per completare l'impostazione dell'attributo. Se le tabelle con titolare obbligatorio contengono per errore dati senza titolare in un sistema multi-tenancy, viene visualizzato un elenco a discesa di dati pubblici nelle tabelle con titolare obbligatorio.

Importante Prima di eseguire `pdm_buildtenant`, è *necessario* configurare il fornitore del servizio.

Per implementare la funzione multi-tenancy, completare la procedura seguente:

1. [Impostare l'opzione Multi-tenancy su "installazione"](#) (a pagina 239) e riavviare CA Service Desk Manager. È necessario avviare i servizi ogni volta che si cambia lo stato del titolare (installazione, attivo, attivo(consenti)).

Importante Quando la funzione multi-tenancy è in modalità installazione, i cambiamenti dell'interfaccia Web sono attivi per gli amministratori del fornitore del servizio, consentendo la visualizzazione e la modifica dei dati e degli oggetti correlati ai titolari nell'interfaccia Web. Non vengono tuttavia applicate le restrizioni di proprietà e gli utenti che non sono amministratori del fornitore del servizio non saranno in grado di visualizzare i cambiamenti dell'interfaccia utente. È pertanto possibile continuare ad utilizzare il prodotto in modalità senza titolare, anche se è configurato per la funzione multi-tenancy.

2. [Associare eventuali implementazioni titolare esistenti all'oggetto titolare.](#) (a pagina 241)
3. [Inserire dati nelle colonne dei titolari](#) (a pagina 242).

Nota: si consiglia di inserire dati nella colonna dei titolari prima nei contatti, quindi di utilizzare i contatti con titolari per inserire dati nella colonna dei titolari degli altri oggetti.

4. Verificare che il titolare sia impostato in tutte le tabelle con titolare obbligatorio.
5. [Creare i titolari.](#) (a pagina 243)

Importante Il primo titolare ad essere creato deve essere il titolare del fornitore del servizio. Dopo aver creato il titolare del fornitore del servizio, disconnettersi da CA Service Desk ed effettuare nuovamente l'accesso come membro del fornitore del servizio. Un modo semplice di eseguire questa operazione consiste nell'effettuare l'accesso come utente con privilegi (ad esempio, ServiceDesk), poiché tale utente appartiene automaticamente al titolare del fornitore del servizio. Se si desidera effettuare l'accesso come un contatto diverso, utilizzare in primo luogo pdm_settenant per assegnare il contatto al fornitore del servizio.

6. [Creare gruppi di titolari.](#) (a pagina 245)

7. [Impostare l'opzione Multi-tenancy su Attivo.](#) (a pagina 239)

Dopo aver selezionato questa opzione, riavviare i servizi e completare i passaggi seguenti:

- a. Effettuare l'accesso utilizzando il nome utente con privilegi (generalmente *ServiceDesk*).
- b. Verificare che l'utente con privilegi venga assegnato al titolare del fornitore del servizio.
- c. Verificare che siano applicate le restrizioni multi-tenancy.

Importante Se i dati senza titolare rimangono nel database, è possibile impostare l'applicazione della funzione multi-tenancy su *Avvisa* o *Consenti*. Ciò consente di aggiornare le tabelle con titolare obbligatorio che non contengono un titolare, evitando così la perdita di dati quando viene attivato un Accordo sui livelli di servizio (SLA) o un evento associato in contrasto con un ticket che non è stato ancora aggiornato in modo da contenere un titolare.

Nota: è possibile eseguire `pdm_settenant` anche dopo che la funzione multi-tenancy è attiva sia per monitorare lo stato dell'implementazione (con l'opzione `-r`), sia per l'aggiornamento di massa del titolare in base alle necessità.

8. Eseguire una copia di backup dei ruoli e dei vincoli partizione dati.

Multi-tenancy semplifica i vincoli partizione dati richiesti riducendone sia il numero che la complessità. Prima di apportare dei cambiamenti, eseguire il backup delle tabelle `Domain_Constraint` e `usp_role`.

9. Rimuovere i vincoli partizione dati non necessari.

Molti vincoli di dominio definiti per titolare unico non sono necessari dopo l'attivazione della funzione multi-tenancy e possono essere rimossi. La rimozione di tali vincoli aggiuntivi consente un miglioramento delle prestazioni.

10. Verificare e controllare.

Eseguire `pdm_settenant -r` per valutare la necessità di aggiungere ulteriori dati relativi ai titolari nelle tabelle con titolare obbligatorio. Valutare la necessità di aggiungere titolari alle tabelle per le quali sono facoltativi, come *Categoria* e *Notifica attività*.

11. (Facoltativo) Disabilitare la funzione multi-tenancy se si verificano problemi. In caso di problemi successivi all'implementazione, è possibile completare i passaggi seguenti:

- a. Ripristinare le tabelle Domain_Constraint e usp_role.
- b. Impostare nuovamente l'opzione Multi-tenancy su "installazione".
- c. Riavviare il sistema.

Il sito può riprendere le operazioni precedenti, anche se si continua ad inserire dati nelle colonne dei titolari e a correggere eventuali problemi che richiedono l'annullamento della modifica.

Nota: se le tabelle con titolare obbligatorio contengono per errore dati senza titolare in un sistema multi-tenancy, viene visualizzato un elenco a discesa di dati pubblici nelle tabelle con titolare obbligatorio e viene visualizzato il messaggio seguente: "AHD05358 xxx oggetti attivi senza titolare *nn* all'avvio di Service Desk".

Abilita Multi-Tenancy

Utilizzando il prodotto, è possibile abilitare la funzione multi-tenancy.

Per abilitare la funzione multi-tenancy

1. Fare clic sulla scheda Amministrazione.
2. Nella struttura a sinistra fare clic su Gestione opzioni, Multi-tenancy.
Viene visualizzata la pagina Elenco opzioni.
3. Fare clic su multi_tenancy.
Viene visualizzata la pagina Dettagli opzioni di multi_tenancy.
4. Fare clic su Modifica.
Viene visualizzata la pagina Aggiorna opzioni.
5. Nell'elenco a discesa Valore opzione selezionare *una* delle opzioni indicate di seguito:

fuori

Disabilita la funzione di multi-tenancy.

configurazione

Abilita la multi-tenancy in modalità configurazione. In questa modalità, CA Service Desk Manager mostra oggetti e attributi modificabili relativi a titolari per amministratori del fornitore di servizi, ma non fa rispettare requisiti di tenancy. Altri utenti possono continuare a lavorare come se la multi-tenancy non fosse installata.

in

Abilita la funzionalità multi-tenancy completa. È possibile scegliere tra i seguenti valori:

- **strict**—(Default) CA Service Desk Manager non realizza un checkin a una tabella che richiede titolare quando il titolare è nullo e il prodotto non può ricavarne l'impostazione predefinita da una tabella titolari SREL.
- **warn**—CA Service Desk Manager scrive un errore nel registro ma permette il checkin quando un oggetto che richiede titolare con titolare nullo viene creato o aggiornato.
- **allow**—CA Service Desk Manager scrive un avviso nel registro ma permette il checkin quando un oggetto che richiede titolare con titolare nullo viene creato o aggiornato.

Nota: se non sono stati inseriti dati nella tabella `ca_tenant`, è necessario selezionare installazione nell'elenco a discesa Valore opzione. Per le nuove implementazioni di multi-tenancy, selezionare installazione.

6. Fare clic su Installa.

L'opzione `multi_tenancy` viene installata.

7. Fare clic su Aggiorna.

Nella pagina vengono visualizzati i cambiamenti.

8. Chiudere la finestra.

Viene visualizzata nuovamente la pagina Elenco opzioni.

9. Riavviare i servizi.

Modalità di inizializzazione di un nuovo titolare

In quanto fornitore del servizio, è possibile creare un set di dati standard per un nuovo titolare, ad esempio categorie, partizioni dati, modelli di ticket e così via. Questa attività può essere eseguita utilizzando `pdm_extract` oppure `pdm_tenant_extract` per creare un file di input `pdm_userload` contenente i dati desiderati.

Se necessario, è possibile modificare questo file con qualsiasi editor di testo. Il file può quindi essere caricato nel database mediante `pdm_userload` con l'argomento `-t` per impostare la colonna dei titolari sul nuovo titolare. Per informazioni sugli argomenti di `pdm_userload` diversi da `-t`, consultare la *Guida all'amministrazione*.

La procedura seguente illustra come inizializzare un nuovo titolare:

1. Creare il titolare nella tabella `ca_tenant`.
Utilizzare la pagina in linea per la [creazione di un titolare](#) (a pagina 243).
2. Caricare i dati standard come descritto precedentemente.
Utilizzare `pdm_userload -t` per impostare il titolare.
3. Creare record di contatto per il nuovo titolare.
Caricare i dati esterni o utilizzare `pdm_userload -t`.

Modalità di conversione di un'implementazione di titolare esistente nell'oggetto titolare

È possibile che siano state utilizzate partizioni dati e un altro oggetto CA Service Desk Manager per ottenere alcune delle funzionalità ora fornite dall'opzione multi-tenancy. Se si desidera convertire un'implementazione in multi-tenancy, il primo passaggio consiste nell'associare i dati dell'oggetto utilizzato precedentemente nel nuovo oggetto titolare. L'oggetto utilizzato precedentemente è denominato *oggetto titolare precedente*. Per la maggior parte dei siti con questi requisiti, l'oggetto titolare precedente è rappresentato dall'oggetto `org` (organizzazione), tuttavia l'approccio seguente può essere utilizzato per qualsiasi oggetto titolare precedente.

1. Se l'oggetto titolare precedente non è `org`, verificare che la rispettiva definizione dell'oggetto Majic specifichi `TENANT_REQUIRED`.
2. Verificare le associazioni degli attributi dall'oggetto titolare precedente al nuovo oggetto titolare nel file `buildtenant.xml` nel percorso seguente:

`$NX_ROOT/samples/multi_tenancy`

Nota: è necessario copiare `buildtenant.xml` nella directory `$NX_ROOT/site/cfg` directory. Inoltre, `buildtenant.xsd` deve trovarsi nella stessa directory di `buildtenant.xml`. In caso contrario, verrà visualizzato un errore. Quando si installa il prodotto, `buildtenant.xsd` si trova in `$NX_ROOT/site/cfg`, quindi non occorre copiare questo file.

Le impostazioni predefinite si basano su `org`. Se l'oggetto titolare precedente non è `org`, è necessario modificare il file.

3. [Eseguire `pdm buildtenant -f`](#) (a pagina 250).
Viene creato un nuovo titolare per ogni oggetto titolare precedente e l'attributo titolare nell'oggetto titolare precedente viene impostato in modo da fare riferimento al nuovo titolare.

4. Accedere a CA Service Desk Manager e rivedere sia l'oggetto titolare sia l'oggetto titolare precedente.

Nota: in alcune situazioni potrebbe essere richiesta l'associazione di più oggetti titolare precedente ad un unico oggetto titolare. Per eseguire questa operazione, aggiornare manualmente gli oggetti titolare precedente interessati, quindi eliminare o disattivare i titolari non utilizzati.

Modalità di inserimento di dati negli attributi titolare nelle tabelle

È possibile inserire dati nell'attributo titolare in un'intera tabella o in un suo sottoinsieme mediante l'utilità *pdm_settenant*. Tale utilità utilizza un file di configurazione per selezionare gli oggetti cui assegnare un titolare e per specificare dove ottenere il titolare per gli oggetti. È possibile specificare un titolare esplicito oppure indicare che il titolare deve essere derivato da un riferimento SREL nell'oggetto cui assegnare il titolare.

Per inserire dati negli attributi titolare delle tabelle mediante *pdm_settenant*, completare i passaggi seguenti:

1. Creare o modificare un file di configurazione.

Il file di configurazione seleziona le righe in cui verranno impostati gli attributi titolare e specifica un'origine per il valore dell'attributo titolare. Il prodotto rende disponibile un file *settenant.xml* di esempio nel percorso seguente:

`$NX_ROOT/samples/multi_tenancy`

Nota: è possibile modificare il file *settenant.xml* di esempio oppure creare un file e copiarlo nella directory `$NX_ROOT/site/cfg`. Inoltre *settenant.xsd* deve trovarsi nella stessa directory di *settenant.xml*. In caso contrario, verrà visualizzato un errore. Quando si installa il prodotto, *settenant.xsd* si trova in `$NX_ROOT/site/cfg`, quindi non occorre copiare questo file.

2. [Esecuzione di *pdm_settenant -f \[file configurazione\] -r*](#) (a pagina 252)

L'utilità *pdm_settenant* legge il proprio file di configurazione ed esegue ciascuna regola definita in sequenza.

Si consiglia di utilizzare prima questa utilità per inserire dati nell'attributo titolare nell'oggetto *cnt* (contatto), quindi di utilizzare l'oggetto *cnt* come origine per inserire dati nel titolare in altri oggetti.

Dopo avere assegnato un titolare appropriato all'oggetto *cnt*, è possibile utilizzarlo come base per l'impostazione del titolare in altre tabelle completando i passaggi seguenti:

- a. Specificare un tag *TenantRule* del tipo="SREL" nel file di configurazione per un attributo con riferimento all'oggetto *cnt* per impostare il titolare in altre tabelle.
 - b. (Facoltativo) Specificare un tag *TenantRule* del tipo="Name" < *nometitolare* > per impostare esplicitamente il titolare in alcune tabelle.
3. Eseguire *pdm_settenant* con un nuovo file di configurazione.
 4. Eseguire nuovamente *pdm_settenant* in base alle necessità.

Dopo avere inserito dati nella colonna dei titolari di un oggetto, è possibile utilizzare i puntatori SREL all'oggetto di interesse come base di un tag *TenantRule* SREL per impostare il titolare in altri oggetti.

Esempio: sintassi del tipo SREL

La sintassi del tipo SREL verifica la presenza di oggetti cnt per i quali non è stato specificato un valore di titolare e utilizza il valore dell'oggetto organizzazione collegato:

```
<Object name="cnt">  
<TenantRule type="SREL">organization</TenantRule>  
<Where>tenant is null</Where>  
</Object>
```

Esempio: sintassi del tipo Name

La sintassi del tipo Name verifica la presenza di oggetti org per i quali non è stato specificato un valore di titolare e imposta il campo del titolare di tali oggetti sul nome di un oggetto Titolare effettivo:

```
<Object name="org">  
<TenantRule type="Name">Tenant A</TenantRule>  
<Where>tenant is null</Where>  
</Object>
```

Creazione di un titolare

È possibile utilizzare il prodotto per creare un titolare.

Per creare un titolare

1. Nella scheda Amministrazione selezionare Gestione protezione e ruoli, Titolari.

Viene visualizzata la pagina Elenco Titolari.

Nota: l'opzione Gestione protezione e ruoli, Titolari è disponibile solo quando la funzione multi-tenancy è installata (in modalità di attivazione o in modalità di installazione).

2. Fare clic su Crea nuovo.

Viene visualizzata la pagina Crea nuovo Titolare.

3. Completare i campi modificabili in base alle esigenze:

Nome

Visualizza il nome del titolare.

Fornitore servizio

Indica se un titolare è fornitore del servizio. Il primo titolare creato è sempre fornitore del servizio.

Numero titolare

(Solo scopo informativo) Visualizza il numero del titolare. Questo campo non viene utilizzato da CA Service Desk Manager.

Stato record

Imposta il titolare sullo stato Attivo o Non attivo.

Titolare padre

Specifica un altro titolare al di sopra di quello in questione che diventa *titolare secondario* in una gerarchia di titolari.

Titolari secondari consentiti

Consente titolari secondari per il titolare. Il titolare non può modificare l'impostazione.

Livello titolare

(Solo scopo informativo) Indica il livello del titolare.

Gruppo Titolari principali

(Solo scopo informativo) Identifica il gruppo dei titolari gestiti dal sistema che contiene questo titolare e tutti quelli al di sopra nella gerarchia di titolari.

Gruppo Titolari secondari

(Solo scopo informativo) Identifica il gruppo dei titolari gestiti dal sistema che contiene questo titolare e tutti quelli al di sotto nella gerarchia di titolari.

Gruppo chiave esterna

(Solo scopo informativo) Identifica il gruppo di titolari gestiti dal sistema che contiene i titolari cui può fare riferimento una SREL nei dati che appartengono a questo titolare. Il gruppo di chiavi esterne è uguale al gruppo di titolari principali.

Gruppo titolare correlato

(Solo scopo informativo) Identifica il gruppo di titolari gestiti dal sistema che è composto dai gruppi di titolari principali e dai gruppi di titolari secondari del titolare.

Condizioni d'uso

Specifica le condizioni d'uso del titolare.

Logo

Specifica l'URL del file del logo del titolare che può essere qualsiasi tipo di immagine Web.

Ubicazione

Visualizza la pagina di ricerca della posizione.

Contatto

Visualizza la pagina di ricerca del contatto.

Nota: se non è associato alcun contatto al rispettivo titolare, i campi Indirizzo di posta elettronica e Indirizzo di posta elettronica cercapersone non sono attivi.

4. Fare clic su Salva.

Viene creato il titolare.

5. Chiudere la finestra.

6. Fare clic con il pulsante destro del mouse sull'Elenco Titolari e scegliere Aggiorna.

L'Elenco Titolari viene aggiornato e visualizza il titolare creato.

7. (Facoltativo) Per assegnare questo titolare ai gruppi di titolari definiti dall'utente, fare clic su Aggiorna gruppi di titolari nella scheda Gruppi titolari.

Creazione di un gruppo di titolari

È possibile utilizzare il prodotto per creare un gruppo di titolari.

Per creare un gruppo di titolari

1. Nella scheda Amministrazione selezionare Gestione protezione e ruoli.
2. Fare clic su Gruppi titolari.

Viene visualizzato l'Elenco Gruppi titolari.

Nota: l'opzione Gestione protezione e ruoli, Gruppi titolari è disponibile solo quando è installata la funzione multi-tenancy (in modalità di attivazione o in modalità di installazione).

3. Fare clic su Crea nuovo.

Viene visualizzata la pagina Crea Nuovo gruppo titolari.

4. Inserire i dati nei seguenti campi:

Nome gruppo titolare

Visualizza il nome del gruppo di titolari.

Stato record

Imposta il gruppo di titolari come attivo o non attivo.

Descrizione

Visualizza una descrizione del gruppo di titolari.

5. Fare clic su Salva.

Il gruppo di titolari viene creato.

6. Chiudere la finestra.
Viene visualizzato l'Elenco Gruppi titolari.
7. Fare clic con il pulsante destro del mouse sull'Elenco Titolari e scegliere Aggiorna.
L'Elenco Gruppi titolari viene aggiornato.
8. Fare clic su Aggiorna titolari nella pagina Dettagli gruppo titolari per aggiungere membri titolari al gruppo.

Gerarchie di titolari

Una *gerarchia di titolari* è un gruppo di titolari strutturato creato dal sistema o modificato quando si assegna a un titolare un *titolare padre*. Il titolare diventa un *titolare secondario* del titolare padre e degli eventuali titolari superiori ad esso nella gerarchia.

Nota: il fornitore del servizio può creare più gerarchie non correlate oppure nessuna gerarchia. Anche in un sistema con gerarchie di titolari, è possibile definire titolari autonomi.

Un titolare secondario rappresenta generalmente una divisione dei rispettivi *titolari principali*. Un titolare secondario può disporre di proprie regole e dati aziendali e i dati del titolare principale sono "inseriti" automaticamente nel titolare secondario in sola lettura.

CA Service Desk Manager supporta gerarchie di titolari di profondità illimitata. Tuttavia, il *fornitore del servizio* può specificare un limite al numero totale di titolari e alla profondità delle gerarchie di titolari (l'impostazione predefinita è quattro livelli). Il fornitore del servizio può inoltre stabilire se singoli titolari possono avere titolari secondari.

Nota: il fornitore del servizio può partecipare alle gerarchie di titolari, ma non obbligatoriamente. Il fornitore del servizio non può avere un titolare padre.

Creazione di un titolare secondario

È possibile creare e modificare gerarchie di titolari a scopi organizzativi e di condivisione dei dati. Per inserire un titolare in una gerarchia di titolari, è necessario assegnarlo a un titolare padre.

Per creare un titolare secondario

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Titolari.

Viene visualizzato l'Elenco titolari.

Nota: l'opzione Gestione protezione e ruoli, Titolari è disponibile solo se è attivata l'opzione multi-tenancy.

2. Fare clic su un titolare esistente da modificare oppure fare clic su Crea nuovo.

Viene visualizzata la pagina Dettagli titolare. Immettere i dati o le modifiche desiderate.

3. Selezionare un titolare padre.

Nota: nell'elenco a discesa dei titolari padre sono visualizzati solo i titolari che possono avere titolari secondari.

4. Fare clic su Salva.

Il titolare è un titolare secondario del titolare padre selezionato.

Nota: quando un titolare è un titolare secondario, appartiene al gruppo Titolari secondari del titolare padre, analogamente agli eventuali titolari secondari del titolare secondario, e così via. Il titolare padre appartiene al gruppo Titolari principali del titolare secondario, analogamente agli eventuali titolari principali del titolare principale, e così via. Ognuno appartiene al gruppo Titolari correlati dell'altro.

Gruppi di titolari gestiti dal sistema

CA Service Desk Manager genera e gestisce automaticamente tre gruppi di titolari per ogni titolare di una gerarchia di titolari (*tenant* è il nome del titolare):

- *tenant_subtenants* (il titolare, i suoi titolari figlio e i loro titolari secondari nella gerarchia)
- *tenant_supertenants* (il titolare, il suo titolare padre e i loro titolari principali nella gerarchia)
- *tenant_relatedtenants* (l'intera singola gerarchia)

I gruppi di titolari gestiti dal sistema possono essere utilizzati come i gruppi di titolari definiti dall'utente. Tuttavia, è possibile modificarne solo il nome e la descrizione.

Modalità di esportazione e importazione di dati di titolari

Il fornitore del servizio può estrarre i dati dei titolari da un'implementazione multi-tenancy esistente e importarli in un nuovo sistema.

Nota: a seconda del volume dei dati, il processo di estrazione può richiedere diverse ore. Potrebbe essere necessario eseguire l'estrazione e l'importazione in più fasi, come indicato di seguito:

Iniziale

Viene estratta una linea di base e viene creato un file di controllo che verrà utilizzato nelle fasi successive.

Aggiorna

Viene utilizzato il file di controllo per estrarre solo i dati che sono cambiati rispetto all'esecuzione precedente.

Finale

Vengono eseguiti gli stessi passaggi di Aggiorna, cui si aggiunge l'estrazione delle animazioni. Le animazioni vengono omesse da entrambe le fasi Iniziale e Aggiorna.

Per estrarre i dati da un database e importarli in un altro database, completare i passaggi seguenti:

1. Eseguire una fase iniziale di [pdm tenant extract](#) (a pagina 256) per estrarre i dati della linea di base. In questo modo viene creato il file di controllo che verrà utilizzato nelle fasi successive.
2. Preparare un nuovo MDB vuoto per i dati estratti.

Importante L'output della fase iniziale *deve* essere caricato in un database che non è mai stato utilizzato per il prodotto o per qualsiasi altro prodotto. Ciascuna tabella caricata dai dati della fase iniziale viene troncata prima del caricamento, il che potrebbe provocare la perdita di dati nel caso in cui il database sia già in uso.

3. Per evitare che nel nuovo sistema vengano visualizzati contatti con privilegi duplicati, è necessario disattivare i contatti con privilegi. Accedere a CA Service Desk Manager e cambiare lo stato di tali contatti in "inattivo" prima di caricare i dati estratti.
4. Per evitare problemi referenziali durante il caricamento dei dati, eseguire lo script di eliminazione dei vincoli appropriato:
 - (Oracle) Eseguire
\$NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql
 - (SQL Server) Eseguire
\$NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql
5. Utilizzare [pdm userload](#) (a pagina 258) per caricare i dati dalla fase iniziale nell'MDB vuoto preparato nei passaggi 2 e 3.
6. Eseguire una fase di aggiornamento o finale di `pdm_tenant_extract` per estrarre dati aggiuntivi creati o modificati rispetto alla fase precedente. `Pdm_tenant_extract` utilizza il file di controllo creato nel passaggio 1 per stabilire quali sono i dati già elaborati dalla fase precedente.
7. Utilizzare `pdm_userload` per caricare i dati estratti nel passaggio 5 nello stesso MDB contenente i dati caricati dalle fasi precedenti.

Nota: per ulteriori informazioni su questa utilità, vedere [pdm userload](#) (a pagina 258).

8. Ripetere i passaggi 5 e 6 in base alle necessità fino ad importare tutti i dati nel nuovo database. L'ultima esecuzione dovrebbe essere la fase finale.
9. Per proteggere l'integrità del nuovo database, ripristinare i vincoli eliminati al passaggio 3 eseguendo lo script di aggiunta vincoli appropriato:
 - (Oracle) Eseguire
\$NX_ROOT/samples/views/Oracle/OracleAddConstraints.sql
 - (SQL Server) Eseguire
\$NX_ROOT/samples/views/SQLServer/SQLAddConstraints.sql
10. Utilizzare [pdm tenant delete](#) (a pagina 255) per eliminare i dati estratti dal database originale.
11. Assicurarsi che tutti i repository associati ai titolari estratti vengano copiati nelle impostazioni di destinazione.

Modalità di gestione di allegati e repository

Gli allegati sono memorizzati nei repository. È necessario copiare nel sistema di destinazione tutti i repository associati ai titolari estratti, inclusi i repository pubblici. Questo processo è un'operazione principalmente manuale che prevede i passaggi seguenti:

1. Ridefinire le informazioni specifiche della posizione per tutti i repository dopo il completamento del caricamento iniziale dei dati nel sistema di destinazione. Questa attività include il cambiamento dei valori seguenti:
 - Nome server
 - Percorso caricamento
 - Percorso servlet
 - Percorso archivio
2. Creare manualmente tutte le directory e le cartelle richieste.
3. Copiare tutti i file allegati dalla posizione precedente nel nuovo percorso di repository dopo (o durante) il caricamento dei dati dalla fase Finale.

Dopo aver completato questi passaggi, tutti i riferimenti per gli allegati nel sistema di destinazione dovrebbero essere eseguiti correttamente. Tuttavia, le copie degli allegati rimangono sul sistema fonte. [Utilizzare l'utilità pdm clean attachments.pl](#) (a pagina 252) per eliminare gli allegati ridondanti.

Utilità utilizzate per la funzione multi-tenancy

In questa sezione vengono descritte le utilità utilizzate per gestire un ambiente multi-tenancy.

Nota: i parametri necessari sono racchiusi tra "{ }", mentre quelli facoltativi tra "[]".

Ulteriori informazioni:

[pdm_buildtenant: creazione di titolari da un altro oggetto](#) (a pagina 250)

[pdm_clean_attachments: eliminazione degli allegati ridondanti dopo l'importazione dei dati del titolare](#) (a pagina 252)

[pdm_settenant: assegnazione di titolari agli oggetti](#) (a pagina 252)

[pdm_tenant_delete: eliminazione dei dati del titolare dal database](#) (a pagina 255)

[pdm_tenant_extract: estrazione dei dati dei titolari](#) (a pagina 256)

[pdm_userload: caricamento dei dati del titolare](#) (a pagina 258)

pdm_buildtenant: creazione di titolari da un altro oggetto

L'utilità *pdm_buildtenant* consente di creare titolari da un altro oggetto. È possibile che siano state utilizzate partizioni dati e un altro oggetto CA Service Desk Manager per ottenere alcune delle funzionalità ora fornite dall'opzione multi-tenancy. Se si desidera convertire un'implementazione in multi-tenancy, il primo passaggio consiste nell'associare i dati dell'oggetto utilizzato precedentemente nel nuovo oggetto titolare mediante *pdm_buildtenant*.

Importante Prima di eseguire *pdm_buildtenant*, è *necessario* configurare il fornitore del servizio.

In questa sezione l'oggetto utilizzato per contenere le informazioni relative al titolare è denominato oggetto titolare precedente. Per la maggior parte dei siti con questi requisiti, l'oggetto titolare precedente è rappresentato dall'oggetto org (organizzazione), tuttavia l'approccio seguente può essere utilizzato per qualsiasi oggetto titolare precedente.

L'utilità *pdm_buildtenant* crea gli oggetti titolare dagli oggetti titolare precedente. Viene creato un nuovo titolare per ogni oggetto titolare precedente e l'attributo titolare nell'oggetto titolare precedente viene impostato in modo da fare riferimento al nuovo titolare. La sintassi di questa utilità è la seguente:

```
pdm_buildtenant [-h] | [-f [file_configurazione]
```

-f file_configurazione

(Facoltativo) Specifica il percorso di un file di configurazione che indica le regole per la creazione di titolari da un oggetto titolare precedente. Se questo argomento non viene incluso, pdm_buildtenant utilizza il file di configurazione dalla directory \$NX_ROOT/site/cfg. L'uso di tale file presuppone che l'oggetto titolare precedente sia org. In caso contrario, è *necessario* modificare il file di configurazione prima di utilizzare pdm_buildtenant.

Nota: è *necessario* copiare buildtenant.xml nella directory \$NX_ROOT/site/cfg. buildtenant.xsd deve inoltre trovarsi nella stessa directory di buildtenant.xml. In caso contrario, verrà visualizzato un errore. Quando si installa il prodotto, buildtenant.xsd si trova in \$NX_ROOT/site/cfg, quindi non occorre copiare questo file.

-h

Visualizza informazioni sull'utilizzo di pdm_buildtenant.

Il formato del file di configurazione è il seguente:

```
<?xml version="1.0" encoding="utf-8" ?>
<BuildTenant>
  <Object from="MajicObjectName">
    <Attribute from="sourceAttribute1" to="tenantAttribute1" />
    <Attribute from="sourceAttribute2" to="tenantAttribute2" />
  </Object>
</BuildTenant>
```

L'attributo *from* del tag Object identifica l'oggetto titolare precedente. Ogni tag Attribute identifica un attributo da copiare dall'oggetto titolare precedente in un attributo del nuovo titolare.

Importante Nelle implementazioni multi-tenancy per UNIX è *necessario* eseguire pdm_task per esportare LIBPATH prima di eseguire le utilità pdm_settenant e pdm_buildtenant. Se non si esegue pdm_task prima di eseguire queste utilità, si riceveranno errori di sistema. Utilizzare ../pdm_task per eseguire il comando.

pdm_clean_attachments: eliminazione degli allegati ridondanti dopo l'importazione dei dati del titolare

Dopo avere importato i dati del titolare, è necessario eliminare gli allegati ridondanti. La sintassi di questa utilità è la seguente:

```
pdm_perl pdm_clean_attachments.pl [-h] [-n repository_name] [-S|-K]
```

-h

Consente di specificare che deve essere visualizzata la Guida della riga di comando.

-n repository_name

Consente di specificare il nome del repository da elaborare. Se questo valore non viene specificato, vengono elaborati tutti i repository.

-S

Consente di specificare che devono essere elaborati solo i repository CA Service Desk Manager.

-K

Consente di specificare che devono essere elaborati solo i repository delle immagini incorporate e Gestione delle informazioni.

Nota: se si esegue il comando `pdm_clean_attachments.pl` senza argomenti, vengono elaborati tutti i repository.

Importante: in UNIX, `LIBPATH` deve essere impostato prima di eseguire diverse utilità di CA Service Desk Manager. Utilizzare `pdm_task` per impostare `LIBPATH` prima di eseguire un'utilità. Immettere ad esempio "`pdm_task pdm_clean_attachments...`".

pdm_settenant: assegnazione di titolari agli oggetti

Dopo aver definito i titolari, utilizzare l'utilità `pdm_settenant` per impostare la colonna dei titolari in altri oggetti. La sintassi di questa utilità è la seguente:

```
pdm_settenant [-h] [-f {configuration_file} [-r]] [-d domsrvr]
```

-d domsrvr

(Opzionale) Specifica un domsrvr da utilizzare. Se questo argomento non è specificato, `pdm_settenant` utilizza il domsrvr predefinito.

-f configuration_file

(Facoltativo) Specifica il percorso di un file di configurazione con indicazione dei dati che verranno aggiornati e delle regole per l'aggiornamento del file. Se questo argomento non viene specificato, pdm_settenant utilizza il file di configurazione nella directory \$NX_ROOT/site/cfg (dopo che il file di configurazione è stato copiato nella cartella NX_ROOT/site/cfg).

Nota: è possibile modificare il file settenant.xml di esempio oppure creare un file e copiarlo nella directory \$NX_ROOT/site/cfg. Inoltre settenant.xsd deve trovarsi nella stessa directory di settenant.xml. In caso contrario, verrà visualizzato un errore. Quando si installa il prodotto, settenant.xsd si trova in \$NX_ROOT/site/cfg, quindi non occorre copiare questo file.

Nel codice XML di esempio seguente viene descritto il formato di questo file:

```
<?xml version="1.0" encoding="utf-8" ?>
<SetTenant>
  <Object name="MajicObjectName">
    <TenantRule type="SREL">MajicColumnName</TenantRule>
    <Where>tenant is null</Where>
  </Object>
  <Object name="MajicObjectName">
    <TenantRule type="Name">TenantName</TenantRule>
    <Where>tenant is null</Where>
  </Object>
</SetTenant>
```

Ogni tag Object specifica un oggetto CA Service Desk Manager cui assegnare un titolare. Il tag TenantRule specifica la modalità con cui pdm_settenant determina il titolare in, mentre il tag Where seleziona gli oggetti cui assegnare il titolare. Sono disponibili due tipi di tag TenantRule:

- tipo="Name"

Specifica un titolare esplicito mediante il nome.

- tipo="SREL"

Specifica un attributo SREL nell'oggetto. Pdm_settenant copia il titolare dell'oggetto cui fa riferimento l'attributo SREL.

-h

Visualizza informazioni sull'utilizzo di pdm_settenant.

-r

Genera un report che visualizza il numero complessivo di righe di ciascuna tabella con titolare obbligatorio e il numero di righe che presentano una colonna che non contiene un titolare.

Nota: se si specifica sia l'argomento -f che -r, pdm_settenant genera un report dopo il completamento dell'aggiornamento. Se si specifica solo l'argomento -r, pdm_settenant genera un report ma non aggiorna i dati.

Se si esegue pdm_settenant senza specificare argomenti, vengono visualizzate le informazioni sull'utilizzo. Per eseguire pdm_settenant utilizzando il file di configurazione predefinito, specificare l'opzione -f senza l'argomento configuration_file. L'utilità pdm_settenant legge il proprio file di configurazione ed esegue ciascuna regola definita in sequenza. Scrive l'output nel file pdm_settenant.log nella directory \$NX_ROOT/log.

È possibile eseguire pdm_settenant tutte le volte che è necessario. Il primo passaggio potrebbe richiedere molto tempo (probabilmente diverse ore per un sito molto grande). Le esecuzioni successive sono più rapide, dato che vengono elaborate solo le righe che non sono state aggiornate. Tale operazione prepara il database prima dell'installazione dell'opzione Multi-Tenancy.

Importante Nelle implementazioni multi-tenancy per UNIX è necessario eseguire pdm_task per esportare LIBPATH prima di eseguire le utilità pdm_settenant e pdm_buildtenant. Se non si esegue pdm_task prima di eseguire queste utilità, si riceveranno errori di sistema. Utilizzare ../pdm_task per eseguire il comando.

Considerazioni sull'assegnazione di titolari agli oggetti

Dopo aver definito i titolari, utilizzare l'utilità pdm_settenant (assegna titolari a oggetti) per impostare la colonna del titolare in altri oggetti. Quando si modifica il titolare per un oggetto, bisogna considerare se modificare la proprietà degli oggetti con titolari correlati al fine di conservare l'integrità dei dati. A causa della mancata sincronizzazione di tali oggetti, è possibile che i dati non vengano visualizzati negli elementi della configurazione, nelle relazioni, nei MDR, nel controllo delle versioni, e così via. I seguenti oggetti CA CMDB presentano un titolare:

- nr—Definizioni degli elementi della configurazione
- nr_com—Voci di registro associate ad un elemento della configurazione
- bmhier—Relazioni associate ad elementi della configurazione
- mdr_idmap—Definizioni del provider MDR
- ci_mdr_idmap—Mapping elemento della configurazione/MDR federati

Per ogni elemento della configurazione, eseguire le operazioni seguenti al fine di sincronizzare i dati quando si utilizza `pdm_settenant` per modificare la proprietà:

- Specificare `nr` per il nome oggetto dell'elemento della configurazione.
- Modificare le voci di registro associate all'elemento della configurazione in `nr_com` in modo tale da poter visualizzare le voci di registro per il nuovo titolare.

Nota: per informazioni sul comando `pdm_settenant`, consultare la *Guida all'amministrazione*.

Esempio: XML per modificare il titolare e il registro

L'XML seguente modifica il titolare per un elemento della configurazione denominato `CITest` in `T2`, come pure le voci di registro corrispondenti in `nr_com`:

```
<TenantRule type="Name">T2</TenantRule>
<Where>name = 'CITest'</Where>
</Object>
<Object name="nr_com">
<TenantRule type="Name">T2</TenantRule>
<Where>asset_id.name = 'CITest'</Where>
\</Object>
```

`pdm_tenant_delete`: eliminazione dei dati del titolare dal database

L'utilità `pdm_tenant_delete` rimuove dal database tutti i dati relativi ad un titolare specificato.

Importante I vincoli referenziali in `ca_tables` devono essere eliminati prima di eseguire `pdm_tenant_delete` e successivamente ripristinati.

La sintassi di questa utilità è la seguente:

```
pdm_tenant_delete -h|-t tenant_name [-C|-R] [-Q]
```

-h

Visualizza le informazioni di utilizzo per `pdm_tenant_delete`.

-t tenant_name

Consente di specificare il nome del titolare dei dati da eliminare.

Nota: per poter utilizzare questa utilità per eliminare i dati, è necessario che il titolare sia contrassegnato come inattivo.

-C

Consente di specificare che tutti i contatti relativi ad un titolare siano contrassegnati come inattivi. Dal momento che è possibile condividere i contatti tra i prodotti, in base alla logica predefinita non si dovrebbero effettuare eliminazioni o disattivazioni di massa dei contatti, a meno che non venga esplicitamente richiesto.

Nota: questa opzione viene ignorata se viene specificata l'opzione -R.

-R

Consente di specificare che tutte le righe di tutte le tabelle con assegnazione dei titolari contrassegnate con CA_COMMON in ddict.sch devono essere eliminate, incluso l'oggetto titolare stesso.

Importante Queste tabelle sono condivise tra più prodotti, pertanto si consiglia di utilizzare questa opzione con attenzione.

-Q

Specifica elaborazioni di query rapide per eseguire query di database il più velocemente possibile. Se questo argomento non è specificato, l'utilità utilizza l'elaborazione di query in background in modo che le query vengono eseguite solo quando il sistema sarebbe inattivo. Questo argomento migliora i tempi di esecuzione a discapito di un maggiore impatto su un sistema attivo.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA Service Desk Manager. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

pdm_tenant_extract: estrazione dei dati dei titolari

L'utilità *pdm_tenant_extract* estrae dal database tutti i dati relativi ad un titolare specificato. Estrae i dati in formato *pdm_userload* per consentirne il corretto caricamento in un altro database. La sintassi di questa utilità è la seguente:

```
pdm_tenant_extract -h | -c control_file [-d domsrvr] [-g yes|no] [-o output_file] -p phase [[-t tenant_name]...] [-Q] [table1 [table2...]]
```

-h

Visualizza le informazioni di utilizzo per *pdm_tenant_extract*.

-c control_file

Specifica il percorso del file di controllo per questa estrazione dei dati relativi al titolare. Per la fase iniziale il file viene creato nel percorso specificato (non deve essere già esistente). Il file deve esistere per le fasi Aggiorna e Finale.

-d domsrvr

(Opzionale) Specifica un domsrvr da utilizzare.

-g yes|no

(Facoltativo) Consente di specificare se i dati pubblici devono essere inclusi nel file di output. Se questo argomento non è specificato, vengono inclusi i dati pubblici di tutte le tabelle.

-o output_file

(Facoltativo) Consente di specificare il percorso del file di output. Se questo argomento non è specificato, l'output viene indirizzato a stdout.

-p phase

Consente di specificare la fase dell'estrazione. Utilizzare uno dei valori seguenti:

I:Iniziale

U: Aggiorna

F: Finale

-t tenant_name

Consente di specificare il nome di un titolare da estrarre. Questo argomento è necessario per la fase iniziale e può essere ripetuto per più titolari. Non è valido per la fase Aggiorna e Finale.

-Q

Specifica elaborazioni di query rapide per eseguire query di database il più velocemente possibile. Se questo argomento non è specificato, l'utilità utilizza l'elaborazione di query in background in modo che le query vengono eseguite solo quando il sistema sarebbe inattivo

table1 [table2...]

(Facoltativo) Consente di specificare le tabelle da estrarre. Se viene omesso, vengono estratte tutte le tabelle.

Importante L'output della fase iniziale deve essere caricato in un database che non è mai stato utilizzato per CA Service Desk Manager o per qualsiasi altro prodotto. Ciascuna tabella caricata dai dati della fase iniziale viene troncata prima del caricamento, il che potrebbe provocare la perdita di dati nel caso in cui il database sia già in uso.

Nota: per evitare problemi referenziali durante il caricamento dei dati, eseguire lo script di eliminazione dei vincoli appropriato (\$NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql oppure \$NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql). Una volta completato il caricamento, applicare nuovamente i vincoli con lo script xxxAddConstraints.sql appropriato che si trova nella stessa directory.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA Service Desk Manager. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

Ulteriori informazioni:

[Modalità di esportazione e importazione di dati di titolari](#) (a pagina 247)

pdm_userload: caricamento dei dati del titolare

L'utilità *pdm_userload* viene utilizzata per caricare i dati in un database CA Service Desk Manager. Questa utilità è disponibile anche se non è installata la funzione multi-tenancy. Tale funzione consente di aggiungere supporto per un argomento aggiuntivo (-t) che specifica il nome di un titolare il cui ID deve essere inserito nella colonna dei titolari di tutte le righe inserite o aggiornate in una tabella con assegnazione dei titolari. È necessario che il titolare specificato sia già incluso nel database.

Quando si estraggono i dati, completare i passaggi seguenti per evitare errori in stdlog:

1. Prima di iniziare a caricare i dati, arrestare CA Service Desk Manager e riavviare il prodotto in modalità DBADMIN come descritto di seguito:

Windows

Eseguire `pdm_d_mgr -s DBADMIN`

UNIX

Eseguire `pdm_init -s DBADMIN`

2. Dopo aver caricato i dati, arrestare CA Service Desk Manager utilizzando il comando `pdm_halt`.
3. Riavviare CA Service Desk Manager in modalità normale.

Nota: per ulteriori informazioni sull'utilità *pdm_userload*, consultare la *Guida all'amministrazione*.

Capitolo 6: Personalizzazione

Questa sezione contiene i seguenti argomenti:

[Panoramica sulla personalizzazione](#) (a pagina 259)

[Personalizzazione del metodo di notifica](#) (a pagina 260)

[Personalizzazione di query e messaggi](#) (a pagina 268)

[Personalizzazione dello schema](#) (a pagina 282)

[Personalizzazione dell'interfaccia Web](#) (a pagina 297)

[Personalizzazione della memorizzazione dei dati del registro eventi](#) (a pagina 387)

[Personalizzazione dei report di CA Business Intelligence](#) (a pagina 389)

[Personalizzazione di rapporti legacy](#) (a pagina 406)

Panoramica sulla personalizzazione

CA Service Desk Manager è un prodotto eccezionalmente flessibile progettato per l'applicazione di varie funzioni di Gestione dei servizi di IT. Il prodotto offre un ampio set di funzionalità e contenuto relativo alle procedure ottimali che consentono di soddisfare le esigenze di gestione dei servizi nel modo più rapido ed esaustivo possibile.

Sebbene l'implementazione predefinita di CA Service Desk Manager sia adatta ai processi e rispetti la terminologia usati nella maggior parte delle organizzazioni IT, può essere necessario estendere il prodotto per coprire tutte le specifiche esigenze di funzionamento delle varie organizzazioni. A tal fine, il prodotto prevede un ampio spettro di approcci per la personalizzazione del prodotto in modo da soddisfare le esigenze specifiche, tra cui:

- Personalizzazione dell'utente finale
- Configurazione a livello di sistema
- Adattamento basato su strumenti
- Personalizzazione a livello di codice

Sono disponibili diversi tipi di approccio per personalizzare il prodotto.

Personalizzazione del metodo di notifica

I metodi di notifica automatica CA Service Desk Manager servono a comunicare informazioni al personale durante i passaggi essenziali del processo di gestione dell'assistenza ai clienti. I metodi di notifica standard sono i seguenti:

- Posta elettronica
- Notifica (registro)
- Posta elettronica cercapersone

È possibile definire metodi di notifica personalizzati per specificare un nuovo metodo di trasmissione, ad esempio posta vocale, bacheche o stampanti specifiche. È possibile anche accedere ai dati da un'altra applicazione e includerli nel messaggio di notifica.

Processo di notifica

Le notifiche dei ticket (applicabili alle questioni, agli ordini di cambiamento e alle richieste) vengono elaborate al momento del salvataggio del ticket, come descritto di seguito:

- Se il metodo di notifica è diverso da Notifica, come Posta elettronica, il processore delle notifiche esegue il metodo di notifica per ogni contatto nell'elenco. Solitamente questo metodo è un file eseguibile o uno script shell, che viene avviato in un nuovo processo. I dettagli sulla notifica vengono memorizzati nelle variabili di ambiente per facilitare l'accesso al file eseguibile/script.
- Per ogni notifica richiesta, il processore delle notifiche imposta le variabili di ambiente NX_NTF_MESSAGE e NX_NTF_SUMMARY utilizzando le informazioni presenti in Titolo messaggio di notifica e Testo del messaggio di notifica, fornite nella pagina Notebook di Modello messaggio della finestra Dettagli notifica attività. Se il destinatario è un contatto valido, vengono create ulteriori variabili di ambiente utilizzando le informazioni presenti nel rispettivo record Dettagli contatto.
- Se per la notifica viene selezionata l'opzione Scrivi su file, viene creato un file di testo con altre informazioni utilizzabili dal metodo di notifica per ottenere ulteriori informazioni dettagliate.
- L'elenco dei contatti che devono ricevere la notifica viene ricavato dalle informazioni fornite nelle pagine Notebook Oggetti, Contatti, Tipi e Indagine della finestra Dettagli notifica attività. Per chi ha un metodo di notifica che corrisponde all'opzione Livello notifica e l'opzione di Gestore opzioni log_all_notify installata, la notifica viene generata prima nel registro notifiche.

Variabili del metodo di notifica

Per il metodo di notifica vengono creati e resi disponibili due set di variabili.

Variabili di ambiente di base

Il primo set di variabili viene creato per ogni notifica inviata, indipendentemente dal fatto che sia stata selezionata l'opzione **Scrivi su file** per la notifica. Queste variabili vengono scritte nell'ambiente come variabili di ambiente e il metodo di notifica vi può accedere nel modo standard. Se si sceglie l'opzione **Scrivi su file** quale metodo di notifica, le variabili vengono scritte anche nel file di notifica, nella sezione delle notifiche.

Le variabili di ambiente seguenti forniscono le informazioni di base sulla notifica. Sono sempre definite, anche se il valore corrispondente non è specificato:

Variabile di ambiente	Descrizione
NX_NTF_MESSAGE	Il testo completo del modello del messaggio, compresa l'espansione di tutte le variabili.
NX_NTF_SUMMARY	L'intestazione completa del modello del messaggio, compresa l'espansione di tutte le variabili.
NX_NTF_URGENCY	L'urgenza della notifica (1 equivale a bassa, 4 è emergenza).

Le variabili di ambiente seguenti vengono create solo se il destinatario è un contatto CA Service Desk Manager valido, nel qual caso vengono impostate usando valori ricavati dal record **Dettagli contatto** del destinatario, come mostrato nella tabella seguente:

Variabile	Campi della finestra Dettagli contatto
NX_NTF_BEEPER_PHONE	N. cercapersone
NX_NTF_COMBO_NAME	Cognome, Nome, Secondo nome
NX_NTF_CONTACT	Contatta ID
NX_NTF_EMAIL_ADDRESS	Indirizzo di posta elettronica o Indirizzo di posta elettronica cercapersone (a seconda del tipo di notifica)
NX_NTF_FAX_PHONE	N. fax
NX_NTF_PUBLIC_PHONE	Numero di telefono

Variabile	Campi della finestra Dettagli contatto
NX_NTF_USERID	ID utente
NX_NTF_VOICE_PHONE	alternativo alternativo

Nota: queste variabili non vengono create se non vengono specificati i valori corrispondenti (con l'eccezione di NX_NTF_CONTACT che non può essere vuota).

Variabili attributo

Il secondo set di variabili, denominato variabili di attributo, è disponibile solo se si seleziona l'opzione Scrivi su file quando si definisce il metodo di notifica. Vengono scritte solo nel file di notifica e non nell'ambiente. Il formato è il seguente:

NX_NTF_attributo[.attributo_secondario]=valore

dove:

attributo

Il nome dell'attributo di cui si vuole ottenere il valore. È il nome dell'attributo definito per l'oggetto. Per un elenco completo di tutti i nomi di attributo per gli oggetti, consultare la Guida di riferimento tecnico di CA Service Desk Manager. Gli oggetti comunemente associati alle notifiche sono i ticket, il cui nome dipende dal tipo di ticket, ad esempio cr per le richieste, e dal contatto che identifica il destinatario, il cui nome oggetto è cnt. Ad esempio, la variabile di ambiente per l'attributo descrittivo di un ticket può avere il formato seguente nel file di notifica:

NX_NTF_DESCRIPTION=Descrizione di esempio.

attributo_secondario

Se il primo *attributo* è un identificativo interno di un altro oggetto, spesso viene aggiunto un attributo secondario per fornire ulteriori informazioni utili tramite la notazione a punti. In termini di database, l'attributo è una chiave esterna che punta a una riga di un'altra tabella invece che un semplice valore di dati. Infatti l'uso di una chiave non elaborata avrebbe poco significato. Per comodità, molti di questi tipi di campo sono già risolti. In tal caso, *attributo_secondario* sarà il valore nella tabella a cui si fa riferimento. Ad esempio, invece di scrivere il valore per l'attributo *assignee*, che è effettivamente memorizzato come l'ID univoco del record del contatto per l'assegnatario, viene scritto il nome combinato dell'assegnatario facendo riferimento all'attributo *combo_name* per l'oggetto *contact*, come mostrato nell'esempio seguente:

```
NX_NTF_ASSIGNEE.COMBO_NAME=Armstrong, Beth
```

Se un attributo non ha un valore, il valore corrispondente di solito è (NULL) o vuoto. Ad esempio:

```
NX_NTF_CALL_BACK_DATE=(NULL)
```

```
NX_NTF_GROUP.COMBO_NAME=
```

Nota: una variabile attributo che esiste sia per il ticket che per il destinatario è *NX_NTF_ID* (l'attributo *id*), che è l'ID univoco del database per l'oggetto.

File di notifica

Se si seleziona l'opzione *Scrivi su file* quando si definisce un metodo di notifica, tutte le variabili di attributo e di ambiente di base vengono scritte in un file di testo che viene chiuso prima di eseguire lo script o il programma del metodo di notifica. Questo file di notifica viene scritto ogni volta che il metodo di notifica viene richiamato per un contatto e costituisce un comodo meccanismo per passare allo script di notifica le informazioni pertinenti altrimenti non disponibili nell'ambiente.

Il percorso completo del file di notifica è impostato nella variabile di ambiente *NX_NTF_FILENAME*, disponibile per il processo di elaborazione del metodo di notifica. Il nome file viene anche aggiunto alla fine del valore immesso nel campo *Metodo di notifica* quando si definisce il metodo. Ad esempio, se il metodo di notifica è *'pdm_perl -w mymethod.pl'*, il processo di elaborazione effettivo eseguirà *'pdm_perl -w mymethod.pl nome_file_notifica_univoco'*.

Importante L'amministratore può eliminare i file di notifica. Questa operazione è importante soprattutto quando un'azienda usa un elevato volume di notifiche che possono generare migliaia di file di notifica al giorno. I file si trovano nella directory temporanea standard (TEMP in Windows e TMP in UNIX). Si consiglia di eliminare il file alla fine dell'esecuzione dello script/programma del metodo di notifica.

Il file di notifica è un file di testo standard diviso in sezioni. Ogni riga contiene una coppia attributo/valore o un indicatore di sezione. Ogni file di notifica contiene tre sezioni, come descritto di seguito. Tutte le sezioni iniziano con i caratteri "-----", seguiti da una riga nuova.

SECTION=obj, dove obj identifica il tipo di oggetto del ticket

Iss

Fornisce informazioni sulla questione.

Chg

Fornisce informazioni sull'ordine di cambiamento.

Cr

Fornisce informazioni sulla richiesta.

SECTION=cnt

Fornisce informazioni sul destinatario.

SECTION=notification

Fornisce le stesse informazioni disponibili nelle variabili di ambiente di base.

Nota: i nomi delle sezioni per il ticket e il destinatario sono i nomi degli oggetti per gli attributi della sezione specifica. Per un elenco completo di tutti i nomi attributo per gli oggetti, vedere la *Guida di riferimento tecnico di CA Service Desk Manager*.

In ogni sezione sono contenute diverse righe di coppie attributo/valore, ognuna delle quali rappresenta un attributo dell'oggetto corrispondente. Le variabili di attributo di questa sezione forniscono informazioni dettagliate sulla formattazione e sul significato di queste righe.

Le interruzioni di riga in un valore di attributo vengono riprodotte come nuove righe nel file di notifica. Il processo di elaborazione del metodo di notifica può utilizzare solo le righe attributo o valore che iniziano con NX_NTF e gli indicatori di sezione. Prima di utilizzare un file di notifica nel processo di elaborazione del metodo di notifica, generare un file di esempio e verificarne il contenuto.

Ulteriori informazioni:

[Variabili di ambiente di base](#) (a pagina 261)

[Variabili attributo](#) (a pagina 262)

Utilizzo di script Perl

La maggior parte dei metodi di notifica richiama un file eseguibile o uno script shell per leggere le variabili di ambiente e inviare il messaggio. Questo procedimento funziona bene nella maggior parte dei server UNIX, mentre esistono delle difficoltà nel leggere le variabili di ambiente in un server Windows.

È possibile usare uno script Perl per superare i problemi di ambiente in Windows. CA Service Desk Manager prevede l'installazione dell'interprete Perl denominato `pdm_perl`. Qualsiasi script Perl richiamato con `pdm_perl` come metodo di notifica può ottenere in modo affidabile le variabili di ambiente. Lo script Perl può leggere e formattare i valori delle variabili di ambiente e proseguire con il resto della notifica, ad esempio chiamare un cercapersone o inviare un messaggio di posta elettronica.

Per i server Windows, è possibile utilizzare l'utilità `launchit`. Una delle funzioni di questa utilità è richiamare gli script o i programmi in un ambiente shell simile al prompt dei comandi con il set di variabili di ambiente appropriato.

Ad esempio, se si scrive uno script Perl chiamato `read_env.pl` per leggere diverse variabili di ambiente descritte in questa guida, è possibile richiamarlo per una notifica immettendo quanto segue nel campo Metodo di notifica della finestra Dettagli metodo di notifica:

```
pdm_perl script_path/read_env.pl
```

Questo metodo di notifica avvia l'interprete Perl ed esegue le istruzioni nello script `read_env.pl`.

Modalità di creazione di un metodo di notifica personalizzato

Per creare un metodo di notifica personalizzato, completare i passaggi seguenti:

1. Creazione di uno script per elaborare il modello del messaggio e trasmetterlo al destinatario. Lo script può essere qualsiasi file eseguibile, a seconda della piattaforma. Possono-essere usati anche interpreti di terzi o di dominio pubblico. Generalmente, in UNIX vengono usati script della shell Bourne, mentre in Windows file `.bat`. Se lo script richiede un modello speciale, è necessario crearlo.
2. Aggiunta di un nuovo metodo di notifica locale mediante l'interfaccia Web.

Ulteriori informazioni:

[Creazione di uno script](#) (a pagina 266)

[Aggiunta del metodo di notifica](#) (a pagina 266)

Creazione di uno script

Attenersi alla procedura seguente per creare uno script del metodo di notifica:

1. Stabilire la modalità di distribuzione della notifica (ad esempio stampata con una stampante particolare).
2. Stabilire il contenuto del messaggio di notifica.
3. Specificare quali informazioni del modello di messaggio devono essere incluse nella notifica.
4. Impostare uno script per trasmettere la notifica.
5. Inserire lo script in un file eseguibile nel percorso del server CA Service Desk Manager.

Aggiunta del metodo di notifica

Dopo aver creato uno script, è necessario definire il nuovo metodo di notifica per CA Service Desk Manager. È possibile aggiungere un metodo di notifica in due modi:

- Utilizzando l'interfaccia Web
- Utilizzando uno script shell UNIX

Ulteriori informazioni:

[Aggiunta del metodo di notifica utilizzando l'interfaccia Web](#) (a pagina 266)
[Aggiunta di un metodo di notifica utilizzando uno script shell UNIX](#) (a pagina 267)

Aggiunta del metodo di notifica utilizzando l'interfaccia Web

Per aggiungere un metodo di notifica utilizzando l'interfaccia Web

1. Fare clic su Metodi notifica da Notifiche nell'Interfaccia di amministrazione.
Viene visualizzato l'elenco Metodo di notifica.
2. Fare clic sul pulsante Crea nuova.
Viene visualizzata la finestra Crea nuovo metodo di notifica.
3. Immettere i dati nei seguenti campi:

Simbolo

(Obbligatorio) Identificare il metodo di notifica.

Scrivi su file

Selezionare questa casella di controllo per scrivere su file le informazioni di contesto del metodo di notifica.

Descrizione

Descrivere il metodo di notifica.

Metodo di notifica

Specificare il percorso completo dello script eseguibile per il metodo di notifica. Se lo script o il programma può essere risolto utilizzando il percorso di sistema, non è necessario specificare il percorso completo. Per un server Windows, è possibile usare l'utilità launchit.exe per richiamare lo script o il programma.

Nota: per ulteriori informazioni sull'utilità launchit, vedere la *Guida in linea*.

Nota: poiché il metodo di notifica viene eseguito dal server CA Service Desk Manager, è necessario inserire lo script del metodo di notifica in una directory a cui sia possibile accedere dal percorso sul server o specificare il percorso completo dello script. In UNIX, a seconda della shell in esecuzione, è possibile eseguire questa verifica eseguendo il comando:

```
which nome_percorso_script
```

Se si verificano problemi con i metodi di notifica, esaminare i registri nella directory \$NX_ROOT/log in UNIX o \$NX_ROOT\log in Windows.

Aggiunta di un metodo di notifica utilizzando uno script shell UNIX

Nel passaggio seguente viene creato uno script shell del metodo di notifica che invia il messaggio di notifica alla stampante dell'assistenza clienti, SDPR2. In questo esempio il messaggio di notifica è costituito dall'intestazione e dal testo del modello di messaggio:

1. Configurare lo script della shell per comporre il testo di notifica e trasmetterlo, come segue:

```
#!/bin/sh  
  
echo "  
  
TO:    $NX_NTF_USERID  
  
SUBJECT: $NX_NTF_SUMMARY  
  
MESSAGE:  
  
$NX_NTF_MESSAGE" |lp -dSDPR2
```

2. Denominare il file eseguibile sd_print e inserirlo in una directory qualsiasi usata per gli script comuni in locale, ad esempio /usr/local/netbin.
3. Rendere eseguibile lo script della shell usando il comando chmod.
4. Fare clic su Metodi notifica da Notifiche nell'Interfaccia di amministrazione.
5. Scegliere Nuovo dal menu File.

6. Immettere i dati in questi campi:

Simbolo

SDPR2

Descrizione

Invia una notifica di backup alla stampante dell'assistenza clienti
SDPR2

Metodo di notifica

/usr/local/netbin/sd_print

7. Fare clic sul pulsante Salva per salvare il nuovo record. Quindi fare clic su Chiudi finestra per chiudere la finestra dei dettagli.

Personalizzazione di query e messaggi

CA Service Desk Manager fornisce numerose funzioni che permettono di restringere l'ambito delle informazioni e quindi concentrarsi su richieste, ordini di cambiamento e questioni pertinenti alla situazione attuale. Una di queste funzioni memorizza le query che è possibile utilizzare per visualizzare informazioni pertinenti nel contatore delle interfacce di amministrazione client o Web. Un'altra funzione consente di personalizzare i messaggi che informano il personale delle attività relative ai ticket.

Le query memorizzate possono evidenziare i ticket correlati all'utente-connesso e personalizzare i campi del contatore nell'area contatore delle interfacce di amministrazione e Web. È possibile personalizzare i messaggi di notifica delle attività in modo che includano gli attributi degli oggetti del registro attività e informazioni su specifici ticket.

Query del segnapunti

Una delle tabelle nel database, Cr_Stored_Queries, definisce le query memorizzate. Queste query, che sono molto simili alle query SQL, possono essere usate per personalizzare i campi contatore sui nodi nell'area contatore delle interfacce di amministrazione e Web. I campi contatore indicano quanti record soddisfano la query. Ad esempio, possono indicare quanti tipi diversi di richieste sono stati assegnati all'utente-collegato.

Ciascun utente può personalizzare i campi del contatore che compaiono nel loro contatore (come spiegato nella guida in linea.) Tuttavia, l'amministratore di sistema deve prima definire vari tipi di richieste che possono essere contati in questi campi del contatore come query memorizzate. Per informazioni sulle query del contatore, vedere la *Guida all'amministrazione*.

Nota: i calcoli del contatore risulteranno errati se i valori delle query del database sono nulli. Ad esempio, se la query del segnapunti specifica che assignee.organization = xyz, e in un record un campo assignee è vuoto (NULL), il record non rientrerà nel calcolo del segnapunti.

Query memorizzate per l'utente collegato

Due dei campi che devono essere definiti nella finestra Dettagli query memorizzata sono Clausola Where e Etichetta. Entrambi questi campi possono contenere espressioni personalizzate per l'utente-collegato. Le query memorizzate fanno riferimento a oggetti e attributi invece che a nomi di tabelle e colonne. Una query memorizzata, personalizzata per l'utente-collegato, è composta da due parti:

L'oggetto (ad esempio cr per una richiesta)

Di solito è specificato a sinistra del segno di uguale (=). La sintassi di questa parte della query memorizzata è:

`nome_attr[.nome_attr...].SREL_nome_attr`

Una query memorizzata ha sempre un tipo, che è il nome dell'oggetto su cui viene eseguita e fornisce il contesto per la query. Nella sintassi precedente, il primo nome_attr deve essere il nome di un attributo dell'oggetto context.

L'utente-collegato (l'istanza dell'oggetto cnt per l'utente)

Deve essere specificato a destra del segno di uguale (=) se i ticket devono essere selezionati in base a un attributo dell'utente-collegato. La sintassi di questa parte della query memorizzata è:

`@nome_attr[.nome_attr...].nome_attr_SREL`

Nota: per ulteriori informazioni su oggetti e attributi, vedere la *Guida di riferimento tecnico di CA Service Desk Manager*.

Sintassi per l'oggetto cr

Usare questa sintassi se il riferimento è all'oggetto richiesta (cr):

nome_attr[.nome_attr...].SREL_nome_attr

Questo esempio identifica l'ubicazione della persona assegnata per gestire un ticket. Il nome dell'oggetto è stato omissso in quanto il tipo della query memorizzata implica l'oggetto cr:

`assignee.location=@cnt.location AND active=1`

assegnatario

È l'attributo nell'oggetto richiesta associato al campo assignee nella tabella corrispondente. Ad esempio, l'attributo assignee è definito nell'oggetto cr con SREL agt, che significa che fa riferimento al factory agt. Il factory agt è parte della definizione dell'oggetto cnt.

ubicazione

È l'attributo nell'oggetto cnt associato al campo c_l_id nella tabella Contatto. L'attributo location è definito nell'oggetto cnt con SREL loc, che significa che fa riferimento all'oggetto loc.

Clausola WHERE

L'esempio seguente mostra un valore che può essere codificato in una clausola WHERE:

`assignee.location=@cnt.location AND active=1`

Dato che il tipo di query memorizzata è una richiesta, questa query seleziona tutte le richieste attive in cui l'ubicazione dell'assegnatario è la stessa dell'utente-collegato.

Etichetta

Gli attributi dell'oggetto cnt possono essere inclusi in etichette allo stesso modo in cui vengono inclusi nelle clausole WHERE. Ecco un esempio dell'uso di un attributo nell'oggetto cnt in un'etichetta:

`@cnt.location.name Calls`

Questa etichetta include il nome di una posizione, ad esempio, Phoenix, in cui Phoenix sostituisce @cnt.location.name quando l'etichetta viene visualizzata in una finestra. L'etichetta verrà visualizzata come Chiamate Phoenix.

Parola chiave IN

La parola chiave IN consente a una query memorizzata di fare riferimento a due o più tabelle senza creare un'unione. Questo potrebbe produrre notevoli efficienze nell'esecuzione della query. Viene codificata nel modo seguente:

```
nome_attr_SREL IN ( valore1 [, valore2 [...]] )
```

Ad esempio, una query di una richiesta potrebbe essere codificata così:

```
category.sym IN ('\Soft%', '\Email')
```

Si ottiene la clausola SQL WHERE seguente:

```
category IN (SELECT persid FROM prob_ctg WHERE sym LIKE 'Soft%' OR sym = 'Email')
```

Uno degli utilizzi della clausola IN è evitare i prodotti cartesiani. Ad esempio, la query seguente genera un prodotto cartesiano estremamente inefficiente:

```
assignee.last_name LIKE 'MIS%' OR group.last_name LIKE 'MIS%'
```

Usando la parola chiave IN, la query non crea un prodotto cartesiano; infatti non crea nessuna unione, come illustrato dall'esempio seguente:

```
assignee.last_name IN 'MIS%' OR group.last_name IN 'MIS%'
```

Nota: le parentesi che in genere racchiudono l'elenco di valori sul lato destro di IN possono essere omesse se è presente un solo valore nell'elenco. Analogamente, è opportuno evitare le unioni nelle partizioni dati convertendo una partizione dati, come illustrato di seguito:

```
assignee.last_name LIKE 'Smith'
```

a:

```
assignee = U'374683AA82ACE34AB999A042F3A0BA2E'
```

dove:

U

indica che il valore è un UUID.

'374683AA82ACE34AB999A042F3A0BA2E'

I 32 caratteri racchiusi tra apici indicano la rappresentazione come stringa di un UUID esistente.

Questo impedisce l'unione ma rende la partizione meno chiara. Usando la parola chiave IN, la stessa partizione può essere scritta come illustrato nell'esempio seguente, che riunifica la chiarezza della prima versione e quasi la stessa efficienza della seconda versione:

```
assignee.last_name IN 'Smith'
```

CA Service Desk Manager supporta l'applicazione della clausola IN negli elenchi QREL o BREL. Ad esempio, se si desidera trovare tutte le richieste in cui gli asset siano i padri di un altro asset specifico (con ID 374683AA82ACE34AB999A042F3A0BA2E), la clausola WHERE appropriata sarà:

```
affected_resource.[parent]child_hier.child IN  
(U'374683AA82ACE34AB999A042F3A0BA2E')
```

La prima parte della clausola, *affected_resource*, è uno SREL (chiave esterna) dell'oggetto cr (richiesta) che punta alla tabella Network_Resource. La parte *child_hier* è l'elenco degli oggetti hier che puntano alle relazioni gerarchiche. L'ultima parte, *child*, costituisce la prima parte della clausola WHERE per la query secondaria IN. La parte 374683AA82ACE34AB999A042F3A0BA2E è il valore della chiave esterna che deve corrispondere a *child*. *[parent]* specifica il valore restituito dalla query secondaria. Poiché il valore id è una rappresentazione come stringa di un UUID, deve essere indicato come tale e scritto così: U'374683AA82ACE34AB999A042F3A0BA2E'.

Di seguito è riportato un esempio del codice SQL effettivamente generato, che restituisce tutte le richieste in cui l'Asset è il padre di un Asset specifico:

```
SELECT Call_Req.id FROM Call_Req WHERE Call_Req.affected_rc IN (SELECT hier_parent FROM  
Asset_Assignment WHERE hier_child = U'374683AA82ACE34AB999A042F3A0BA2E')
```

Per eseguire query su più padri, è possibile specificare un elenco separato da virgole nella parte () dell'SQL, come mostrato nell'esempio seguente:

```
affected_resource.[parent]child_hier.child IN (U'374683AA82ACE34AB999A042F3A0BA2E',  
U'374683AA82ACE34AB999A042F3A0BA2E')
```

Il nome dell'attributo tra parentesi quadre ([]) è usato per creare la parte SELECT della clausola secondaria. La notazione con parentesi quadre non è usata per le query memorizzate fornite con Unicenter Service Desk 6.0, come illustrato in questo esempio:

```
(assignee = @cnt.id OR group.group_list.member IN (@cnt.id)) AND active = 1
```


Nota: se non si usa la notazione con le parentesi quadre, il sottosistema SQL presuppone che il nome dell'attributo sia il primo simbolo nella parte con la notazione a punti. In questo caso, l'oggetto group_list contiene l'attributo 'group'. Se fosse richiamato da un'altra parte, l'analisi della clausola WHERE non riuscirebbe! La clausola equivalente con le parentesi quadre è illustrata di seguito:

```
(assignee = @cnt.id OR group.[group]group_list.member IN (@cnt.id)) AND active = 1
```

Nota: non è possibile estendere la notazione a punti. Ad esempio, il caso seguente non è valido:

```
affected_resource.[parent]child_hier.child.name IN ('chicago1')
```

Query basate sulla priorità

Nel database la tabella Priority ha due colonne: sym ed enum. Gli utenti vedono i valori della colonna sym. L'applicazione invece vede i valori della colonna sym in base ai valori della colonna enum. Attualmente, i valori sym predefiniti da 1 a 5 hanno i rispettivi valori enum invertiti.

Esempio

Simbolo	Enumerazione
1	5
2	-4
3	3
-4	2
5	1

Pertanto, quando si scrive una query memorizzata e si fa riferimento al valore 5, in effetti si sta cercando la priorità 1, a meno che non si usi .sym per specificare l'attributo da cercare.

Importante Non cambiare i valori di enumerazione predefiniti assegnati dal prodotto. Se si aggiungono nuovi valori sym, è sufficiente proseguire dal valore enum più alto.

Query basate sul tempo

Per creare query basate sul tempo, è possibile usare periodi di tempo. Un periodo di tempo può essere relativo alla data corrente. Ad esempio, un periodo di tempo potrebbe fare riferimento a oggi, ieri, la settimana scorsa o il mese scorso. Un periodo di tempo ha un nome, ad esempio OGGI o IERI. In una query memorizzata è possibile fare riferimento a un periodo di tempo usando una delle due funzioni incorporate:

StartAtTime (nome-periodo)

In questo modo si fa riferimento all'inizio dell'intervallo definito dal periodo di tempo.

EndAtTime (nome-periodo)

In questo modo si fa riferimento alla fine dell'intervallo definito dal periodo di tempo.

Le regole della sintassi per le query memorizzate richiedono che il nome del periodo sia racchiuso tra apici e che ogni apice sia preceduto da una barra rovesciata. Ad esempio, per fare riferimento all'inizio della settimana scorsa, specificare:

```
StartAtTime('\\SETTIMANA_SCORSA\\')
```

Il trascorrere del tempo rende necessario aggiornare periodicamente una query memorizzata che contiene un riferimento a un periodo di tempo. Ad esempio, l'intervallo descritto da "ieri" cambia a mezzanotte. Nella finestra Dettagli periodo, è possibile specificare Ora di avvio, Ora di fine e Ora trigger per gli aggiornamenti.

Ora di avvio

Ora di avvio specifica l'inizio del periodo di tempo in termini assoluti o relativi. La tabella seguente descrive i campi nella sezione Ora di avvio della finestra Dettagli periodo:

Anno

Un anno esplicito, ad esempio 2000, o un anno relativo, ad esempio +1 (anno successivo) o -1 (anno precedente)

Mese

Un mese esplicito da 1 (gennaio) a 12 (dicembre) o un mese relativo, ad esempio +1 (mese successivo) o -1 (mese precedente)

Giorno

Un giorno esplicito da 1 a 31 o un giorno relativo, ad esempio +1 (domani) o -1 (ieri)

Ora

Un'ora esplicita da 0 a 24 o un'ora relativa, ad esempio +1 (ora successiva) o -1 (ora precedente)

Minuti

Un minuto esplicito da 0 a 59 o un minuto relativo, ad esempio +1 o -1

Ora di fine

Ora di fine specifica la fine del periodo di tempo in termini assoluti o relativi. I campi Ora di fine della finestra Dettagli periodo sono uguali ai campi Ora di avvio della stessa finestra.

Ora trigger

Il campo Ora trigger specifica quando la clausola WHERE di una query memorizzata contenente un riferimento al periodo di tempo viene creata nuovamente e la query memorizzata viene aggiornata. L'ora trigger deve essere relativa all'ora corrente, come descritto nella tabella seguente:

Anno

Deve essere un anno relativo da -1 (anno precedente) a +36 (fra 36 anni).

Mese

Deve essere un mese relativo da -1 (mese precedente) a +11 (fra 11 mesi).

Giorno

Deve essere un giorno relativo da -1 (ieri) a +31 (fra 31 giorni).

Ora

Deve essere un'ora relativa da -1 (ora precedente) a +23 (fra 23 ore).

Minuti

Devono essere minuti relativi da +9 (fra 9 minuti) a +59 (fra 59 minuti).

Query specifiche di ITIL

I problemi e gli incidenti sono semplicemente delle richieste con un determinato valore nell'attributo *type*: "I" per gli incidenti e "P" per i problemi.

La query memorizzata seguente elencherà tutti gli incidenti in cui l'organizzazione dell'assegnatario o del gruppo è uguale all'organizzazione degli analisti collegati:

```
assignee.organization IN @cnt.organization OR group.organization IN @cnt.organization) AND active = 1 AND type = 'I'
```

Per i problemi, la query è identica tranne che per il tipo, ovvero 'P'

Personalizzazione dei messaggi di notifica delle attività

I messaggi di notifica possono essere inviati automaticamente quando si verificano attività di richiesta.

Nota: per informazioni sui messaggi di notifica e sulle istruzioni per definire le notifiche attività, consultare la *Guida all'amministrazione*.

Due dei campi che devono essere definiti nella finestra Dettagli notifica attività sono Titolo messaggio di notifica e Testo del messaggio di notifica. Entrambi questi campi possono contenere attributi ricavati dall'oggetto registro attività (alg per Richieste/Incidenti/Problemi, chgalg per ordini di cambiamento e issalg per questioni). Questi tre oggetti sono quasi identici e possono identificare la richiesta specifica relativa all'attività.

Formattazione degli attributi per le notifiche delle attività

Usando le proprietà elencate di seguito, è possibile definire formattazione e escape opzionali di singoli attributi. Ciò può essere utile soprattutto per formattare le notifiche HTML in cui può essere necessario sostituire i dati nell'attributo per soddisfare gli standard HTML.

Per includere la formattazione, usare la sintassi seguente:

```
@{property=value property=value:attribute_name}
```

Le coppie di valori delle proprietà devono essere separate da almeno uno spazio; è possibile usare indifferentemente maiuscole e minuscole. Un segno di due punti separa le proprietà di formattazione dal nome dell'attributo. Se non sono elencate proprietà, sull'attributo non verrà applicata nessuna formattazione o escape.

Di seguito sono riportate le proprietà di formattazione disponibili:

Proprietà	Descrizione
DATE_FMT	Specifica il formato della data per l'attributo. I valori validi sono: MM/DD/YYYY MM-DD-YYYY DD/MM/YYYY DD-MM-YYYY YYYY/MM/DD YYYY-MM-DD Valida solo per gli attributi della data. Non ha effetti sulle stringhe incorporate nelle date.
ESC_STYLE=NONE HTML URL	Specifica il tipo di escape del testo formattato. I valori validi sono: NESSUNO Impostazione predefinita. Specifica che non verrà applicato alcun trattamento speciale a nessun carattere nel corpo del contenuto. HTML Applica un trattamento speciale ai caratteri seguenti, che hanno significato nel testo HTML: ■ & diventa &amp; ■ " diventa &quot; ■ < diventa &lt; ■ > diventa &gt;

Proprietà	Descrizione
	URL Converte tutti i caratteri diversi da lettere, cifre e '@*-_.#' in '%xx', dove xx è la codifica esadecimale del carattere convertito.
JUSTIFY=LEFT CENTER RIGHT TRUNCATE WRAP LINE	TRUNCATE Valore predefinito nel caso della formattazione. Tronca il testo al valore indicato dalla proprietà WIDTH se si tratta di un numero intero positivo. Se si specifica ESC_STYLE=HTML, viene eliminata la formattazione HTML mediante la sostituzione di '<' e '>' con < e > (vedere KEEPLINKS e KEPTAGS). LEFT CENTER RIGHT Produce esattamente i caratteri indicati da WIDTH, applicando troncamento o riempimento con spazi se necessario, e sostituisce eventuali righe nuove incorporate con un solo spazio. Se si specifica ESC_STYLE=HTML, il testo di output è delimitato dai tag [set the pre variable for your book] e </pre>. L'argomento WIDTH deve essere specificato come numero intero positivo. WRAP Come LEFT, tranne per il fatto che il testo viene portato a capo mantenendo intere le parole (le interruzioni di riga non vengono inserite all'interno delle parole). LINE Come TRUNCATE, tranne per il fatto che sostituisce anche tutte le interruzioni di riga incorporate con tag se ESC_STYLE=HTML.
KEEPLINKS=YES NO	Se si specifica KEEPLINKS=YES, l'azione di JUSTIFY=LINE o JUSTIFY=TRUNCATE viene modificata per conservare i tag di ancoraggio HTML (Azione:) mentre converte tutti gli altri caratteri '<' e '>'. KEEPLINKS e KEPTAGS si escludono a vicenda. Valido solo se ESC_STYLE=HTML.
KEEPNL=YES NO	L'azione normale di PDM_FMT consiste nel convertire in uno spazio singolo tutte le nuove righe incorporate e qualsiasi spazio successivo. Se viene specificato KEEPNL=YES, le nuove righe incorporate verranno conservate. Questo argomento è ignorato da JUSTIFY=LINE.
KEPTAGS=YES NO	Se si specifica KEPTAGS=YES, l'azione di JUSTIFY=LINE o di JUSTIFY=TRUNCATE viene modificata per conservare tutti i tag HTML. KEPTAGS e KEEPLINKS si escludono a vicenda. Valido solo se ESC_STYLE=HTML.
PAD=YES NO	Se si specifica PAD=NO, PDM_FMT non converte le stringhe vuote in un singolo spazio. Questa è l'azione normale quando il valore di WIDTH è

Proprietà	Descrizione
	diverso da zero o JUSTIFY è TRUNCATE o WRAP.
WIDTH= <i>nn</i>	Quando il valore è diverso da zero, specifica che il testo deve essere formattato esattamente con i caratteri indicati da WIDTH.

Ad esempio, per formattare la descrizione della richiesta per una notifica HTML sostituendo specifici caratteri HTML, aggiungendo tag
 per le interruzioni di riga e mantenendo tutti i link HTML come tali, specificare quanto segue:

```
@{ESC_STYLE=HTML JUSTIFY=LINE KEEPLINKS=YES:call_req_id.description}
```

Per formattare il campo open_date di una richiesta nella sequenza giorno-mese-anno, specificare quanto segue:

```
@{DATE_FMT=DD-MM-YYYY:call_req_id.open_date}
```

Attributes presi dall'oggetto registro attività

Per includere un attributo dell'oggetto registro attività, inserirlo nel campo Titolo messaggio di notifica o Testo del messaggio di notifica:

```
@{att_name}
```

Il nome dell'oggetto, alg, chgalg o issalg, è il valore predefinito e non è necessario specificarlo. Ad esempio, per includere il tipo di attività nel titolo del messaggio, specificarlo nel campo Titolo messaggio di notifica (insieme alle altre informazioni che si desidera inserire nel titolo):

```
@{type}
```

Per includere la descrizione dell'attività nel testo del messaggio, specificarla nel campo Testo del messaggio di notifica (insieme alle altre informazioni che si desidera inserire nel testo):

```
@{description}
```

Informazioni su specifici ordini di cambiamento

Affinché i messaggi forniscano informazioni sull'ordine di cambiamento specifico che ha attivato la notifica, i campi Titolo messaggio di notifica o Testo del messaggio di notifica devono contenere un attributo dell'oggetto registro attività che faccia riferimento all'oggetto ordine di cambiamento. Inserire il riferimento in questo formato:

```
@{change_id.chg_att_name}
```

In questo riferimento, si applicano le seguenti informazioni:

@

Indica di sostituire questa espressione.

change_id

L'attributo dell'oggetto registro attività che si collega a una specifica istanza dell'oggetto ordine di cambiamento (chg).

nome_attr_chg

Qualsiasi attributo dell'oggetto chg.

Ad esempio, per includere la priorità dell'ordine di cambiamento nel titolo del messaggio, specificare quanto segue nel campo Titolo messaggio di notifica (insieme alle altre informazioni che si desidera inserire nel titolo):

@{change_id.priority.sym}

Per identificare chi ha segnalato l'ordine di cambiamento (utente finale interessato) nel testo del messaggio, specificare quanto segue nel campo Testo del messaggio di notifica (insieme alle altre informazioni che si desidera inserire nel testo):

@{change_id.requestor.combo_name}

Per riaprire un ordine di cambiamento specifico in base al numero e visualizzare un messaggio come quello riportato di seguito, utilizzare la sintassi seguente:

Reopen Change Order @{change_id.chg_ref_num}

Nota: affinché i messaggi forniscano informazioni su una questione che ha attivato la notifica, i campi Titolo messaggio di notifica e Testo del messaggio di notifica devono contenere un attributo dell'oggetto registro attività che faccia riferimento all'oggetto questione (iss). Per effettuare questa operazione, usare le informazioni per le richieste e gli ordini di cambiamento fornite in questa sezione e le informazioni su oggetti e attributi nella *Guida di riferimento tecnico di CA Service Desk Manager*.

Ad esempio, per includere la priorità della questione nel titolo del messaggio, specificare quanto segue nel campo Titolo messaggio di notifica (insieme alle altre informazioni che si desidera inserire nel titolo):

@{issue_id.priority.sym}

Informazioni su specifiche richieste

Affinché i messaggi forniscano informazioni sulla richiesta specifica che ha attivato la notifica, i campi Titolo messaggio di notifica e Testo del messaggio di notifica devono contenere un attributo dell'oggetto registro attività che faccia riferimento all'oggetto richiesta. Specificare il riferimento in questo formato:

@{call_req_id.nome_attr_cr}

@

Indica di sostituire questa espressione.

call_req_id

L'attributo dell'oggetto registro attività che si collega a una specifica istanza dell'oggetto richiesta (cr).

nome_attr_cr

Qualsiasi attributo dell'oggetto cr.

Ad esempio, per includere l'impatto della richiesta nel titolo del messaggio, specificare quanto segue nel campo Titolo messaggio di notifica (insieme alle altre informazioni che si desidera inserire nel titolo):

@{call_req_id.impact.sym}

Per identificare la risorsa interessata nel testo del messaggio, specificare quanto segue nel campo Testo del messaggio di notifica (insieme alle altre informazioni che si desidera inserire nel testo):

@{call_req_id.affected_resource.name}

Per riaprire una richiesta specifica in base al numero e visualizzare un messaggio come quello riportato di seguito, utilizzare la sintassi seguente:

Reopen Request @{call_req_id.ref_num}

Esistono diversi altri tipi di meccanismi per mezzo dei quali è possibile inviare i messaggi, presenti nel contesto della richiesta stessa (o dell'ordine di cambiamento o della questione). Quando il contesto è la richiesta stessa, non è necessario (e non è possibile) usare la parte "call_req_id" del riferimento. Pertanto, in questi casi, è necessario usare:

"@{ref_num}" invece di "@{call_req_id.ref_num}"

Personalizzazione dello schema

È possibile utilizzare Screen Painter Web per modificare lo schema flessibile del database di CA Service Desk Manager in base alle proprie esigenze.

Progettazione schema fornisce un'interfaccia grafica facile da usare per esaminare e modificare lo schema CA Service Desk Manager. Screen Painter Web consente anche di eseguire il test dei cambiamenti dello schema nei propri moduli Web prima di aggiornare lo schema DBMS fisico o di interessare altri utenti con le modifiche.

Di seguito sono riportati i tipi di cambiamento che è possibile apportare allo schema e usare nei propri moduli e report:

- Aggiungere nuove tabelle al database.
- Aggiungere nuove colonne alle tabelle esistenti.
- Rendere obbligatoria una colonna.
- Cambiare il nome visualizzato o un gruppo di funzioni di una tabella o di una colonna

Tenere presenti le considerazioni seguenti prima di utilizzare Screen Painter Web:

- Non è possibile cambiare la lunghezza di una colonna esistente utilizzando Screen Painter Web e si raccomanda di *non* farlo utilizzando altri strumenti. Le modifiche alla lunghezza di una colonna esistente non sono supportate e possono impedire ad altre applicazioni di accedere al database CA Service Desk Manager.

Importante Non abbreviare o eliminare mai un campo esistente. Queste operazioni compromettono il funzionamento di CA Service Desk Manager.

- Quando si aggiungono colonne ad una tabella esistente, fare attenzione a non superare inavvertitamente la lunghezza massima dei record del database sottostante. Controllare le specifiche per il database che si intende utilizzare con CA Service Desk Manager e apportare le modifiche tenendo presenti i limiti di quel database.
- La pubblicazione dei cambiamenti nello schema del database potrebbe comportare brevi o prolungati tempi d'inattività, a seconda della capacità del database.
- Se si è un nuovo utente di CA Service Desk Manager, è più facile apportare tutti i cambiamenti in fase di test invece di aspettare la fase di produzione.
- Rivedere le procedure generali da completare prima e dopo il cambiamento dello schema di database.
- Utilizzare procedure specifiche per personalizzare lo schema. La maggior parte di queste procedure è seguita da un esempio di cambiamento allo schema standard del database.

Importante Screen Painter Web verifica che la prima lettera di un nuovo nome di tabella o colonna sia "z" e inserisce una "z" se necessario. Ciò garantisce che i nomi dei campi definiti dall'utente non entrino in conflitto con quelli usati da CA Service Desk Manager, in questa versione o in quelle successive.

Modalità di modifica di Progettazione schema

Per modificare lo schema di CA Service Desk Manager, realizzare i seguenti passaggi:

1. Apportare i cambiamenti usando Progettazione schema di Screen Painter Web. È possibile sia modificare tabelle e colonne esistenti che definirne di nuove.
2. Inserire i cambiamenti nella modalità di test. I cambiamenti nella modalità di test sono definiti per il motore oggetti associato a Screen Painter Web, ma non per il database fisico. Gli utenti di Screen Painter Web possono accedere allo schema modificato, ma di solito questo non riguarda gli utenti di CA Service Desk Manager.
3. Aggiornare o creare moduli Web usando lo schema modificato. È possibile esaminare i dati nei moduli Web e anche creare o aggiornare i record nelle tabelle definite a livello di sito senza interessare il database CA Service Desk Manager. Tutti gli aggiornamenti interessano solo il motore oggetti associato a Screen Painter Web.
4. Ripetere i passaggi 1 - 3 per completare le modifiche allo schema e i moduli Web che le usano.
5. Pubblicare i cambiamenti allo schema. La pubblicazione richiede di interrompere l'esecuzione di CA Service Desk Manager.

Visualizzazione dello strumento Progettazione schema Screen Painter Web

È possibile apportare cambiamenti a CA Service Desk Manager usando lo strumento Progettazione schema.

Per visualizzare questo strumento:

1. Avviare Screen Painter Web.
 - (Windows) Dal menu Start di Windows scegliere Programmi, CA, CA Service Desk Manager, Screen Painter Web.
 - (UNIX) Immettere il comando `pdm_wsp` with `$NX_ROOT/bin` nel percorso.

Viene visualizzata la finestra di accesso di Screen Painter Web.

2. Immettere nome utente e password.
3. Scegliere Progettazione schema dal menu Strumenti.

Viene visualizzata la finestra Progettazione schema.

La parte sinistra della finestra Progettazione schema mostra il database CA Service Desk Manager in una struttura ad albero. La visualizzazione iniziale elenca le tabelle, ognuna delle quali è preceduta dal segno più (+) e da un'icona di cartella di colore giallo. Per visualizzare le colonne in una tabella, fare doppio clic sul nome della tabella oppure fare clic sul segno più. Il segno più cambia nel segno meno (-) e in Screen Painter Web verranno visualizzate le colonne della tabella in una struttura ad albero.

Le tabelle e le colonne vengono mostrate in sequenza in base al nome oggetto. Inoltre, se il nome visualizzato è differente dal nome oggetto della tabella o della colonna, il nome viene visualizzato tra parentesi dopo il nome oggetto.

La parte destra della finestra visualizza le proprietà della tabella o della colonna selezionata.

Schede di Progettazione schema

Scheda Informazioni tabella

Quando si fa clic su una tabella nella relativa struttura, Screen Painter Web riempie la scheda Informazioni tabella con le informazioni pertinenti. È possibile visualizzare le seguenti informazioni nella scheda Informazioni tabella:

Nome

Il nome oggetto della tabella. Ad esempio, il nome oggetto della tabella cr è "cr". Questo è un campo di sola lettura.

Nome visualizzato

Il nome descrittivo della tabella. Ad esempio, il nome visualizzato della tabella cr è "Richiesta". È possibile modificare il nome visualizzato di una tabella immettendo un nuovo nome in questo campo.

Nome schema

Il nome utilizzato come riferimento alla tabella nelle utilità CA Service Desk Manager, ad esempio pdm_userload. Questo campo è di sola lettura per le tabelle standard. Nelle tabelle definite a livello di sito, per impostazione predefinita il nome dello schema è uguale al nome oggetto. Per cambiare tale nome, immettere un nuovo valore in questo campo.

Nome DBMS

Visualizza il nome utilizzato per fare riferimento alla tabella nel DBMS fisico. Questo campo è di sola lettura per tutti le tabelle. Nelle tabelle definite a livello di sito, è sempre uguale al nome dello schema.

Descrizione

Una breve descrizione della tabella.

Campo visualizzazione predefinito (nome comune)

La colonna visualizzata nell'interfaccia utente per un campo che fa riferimento a questa tabella. Ad esempio, il campo Assegnatario di una richiesta è un riferimento alla tabella Contatto. Poiché il nome comune della tabella Contatto è combo_name (cognome, nome, secondo nome), il nome combinazione del contatto a cui fa riferimento viene mostrato nell'interfaccia utente come il valore dell'assegnatario. Non è possibile modificare il valore del nome comune.

Campo chiave esterna (REL_ATTR)

La colonna memorizzata nel database per un campo che fa riferimento a questa tabella. Ad esempio, il campo Assegnatario di una richiesta è un riferimento alla tabella Contatto. Poiché il valore di REL_ATTR della tabella Contatto è un ID, la colonna assignee di una richiesta conterrà l'ID del contatto a cui fa riferimento. Non è possibile modificare il valore di REL_ATTR.

Gruppo funzioni

Il nome del gruppo che controlla il livello di accesso degli utenti ai record della tabella. Ogni tipo di accesso del contatti specifica se i contatti possono leggere, modificare o accedere ai dati delle tabelle in ogni gruppo di funzioni. È possibile cambiare il valore di REL_ATTR selezionando un nuovo valore dall'elenco a discesa.

Scheda Informazioni colonna

Nella struttura Tabelle, quando si fa clic su una colonna di una tabella, Screen Painter Web riempie la scheda Informazioni colonna con le informazioni relative alla colonna selezionata. È possibile visualizzare le seguenti informazioni nella scheda Informazioni colonna:

Nome

(Solo visualizzazione) Il nome oggetto della colonna. Ad esempio, il nome oggetto della colonna alt_phone della tabella Contatto è "alt_phone".

Nome visualizzato

Il nome descrittivo della colonna. È possibile modificare il nome visualizzato di una colonna immettendo un nuovo nome in questo campo. Ad esempio, il nome visualizzato della colonna alt_phone della tabella Contatto può essere "telefono alternativo".

Nome schema

Il nome usato come riferimento alla colonna nelle utilità CA Service Desk Manager, ad esempio pdm_userload. Questo campo è di sola lettura per le tabelle standard. Nelle tabelle definite a livello di sito, per impostazione predefinita il nome dello schema è uguale al nome oggetto. Per cambiare tale nome, immettere un nuovo valore in questo campo.

Nome DBMS

Visualizza il nome utilizzato per fare riferimento alla tabella nel DBMS fisico. Questo campo è di sola lettura per tutti le tabelle. Nelle tabelle definite a livello di sito, è sempre uguale al nome dello schema.

Descrizione

Una breve descrizione della colonna.

Tipo campo

Il tipo di dati della colonna. Questo campo è di sola lettura per tutte le colonne standard nelle tabelle standard e per le colonne definite in locale che sono state salvate. È possibile specificare o cambiare il tipo di campo delle nuove colonne definite a livello di sito selezionando un valore dall'elenco a discesa. I tipi di campo disponibili sono:

INTEGER

Indica un valore numerico

STRING

Indica una stringa di testo. Il numero di caratteri in una stringa viene mostrato o immesso nel campo Lunghezza stringa.

DATE

Indica la data e l'ora. Il valore memorizzato nel database è un valore intero che indica il numero di secondi a partire dalla mezzanotte del 1 gennaio 1970.

DURATION

Indica un periodo di tempo. Il valore memorizzato nel database è un valore intero che indica un numero di secondi.

DOUBLE

Indica un numero reale (a virgola mobile).

SREL

Indica una chiave esterna che fa riferimento a un'altra tabella. La tabella a cui la chiave fa riferimento è specificata nel campo Tabella SRel. Il valore memorizzato nel database è il valore REL_ATTR della tabella a cui la chiave fa riferimento e può essere un valore intero o una stringa. Il valore memorizzato nel prodotto è il nome comune della riga della tabella a cui la chiave fa riferimento. Per informazioni sull'impostazione degli attributi SREL con i valori chiave esterna, vedere la Guida di riferimento tecnico di CA Service Desk Manager.

BREL

Indica una colonna virtuale che rappresenta un set di tutti gli oggetti con una chiave SREL che fa riferimento a questa tabella. È presente solo nel motore oggetti e non è fisicamente memorizzato nel database. Questo tipo di campo deve essere selezionato solo con la supervisione di un dipendente CA.

QREL

Indica una colonna virtuale che rappresenta un set di oggetti selezionato tramite la clausola WHERE nella scheda Avanzate. È presente solo nel motore oggetti e non è fisicamente memorizzato nel database. Questo tipo di campo deve essere selezionato solo con la supervisione di un dipendente CA.

DERIVED

Indica una colonna virtuale creata dal motore oggetti utilizzando i valori di altre colonne e tramite una formula specificata nella scheda Avanzate. È presente solo nel motore oggetti e non è fisicamente memorizzato nel database. Questo tipo di campo deve essere selezionato solo con la supervisione di un dipendente CA.

Lunghezza stringa

La lunghezza di una colonna di tipo STRING. Questo campo è vuoto per le colonne di tipo diverso da STRING. Questo campo è di sola lettura per tutte le colonne standard e per le colonne definite in locale che sono state salvate. Per specificare o cambiare la lunghezza della nuova colonna di tipo STRING definita in locale, in questo campo immettere un valore intero compreso tra 1 e 32767.

Tabella SRel

La tabella a cui fa riferimento una colonna SREL. Questo campo è vuoto per le colonne di tipo diverso da SREL. Questo campo è di sola lettura per tutte le colonne standard e per le colonne definite in locale che sono state salvate. È possibile specificare la tabella a cui fa riferimento una nuova SREL definita a livello di sito selezionandola dall'elenco a discesa.

Valore predefinito alla creazione

Il valore predefinito assegnato alla colonna quando viene definita una nuova riga della tabella. Deve essere un valore appropriato al tipo di campo. Sono disponibili alcuni valori di parole chiave per determinati tipi di campo:

NOW

Specifica la data e l'ora correnti per una colonna di tipo DATE.

USER

Specifica l'utente attivo per una SREL della tabella Contatto.

Valore impostato al salvataggio

Il valore assegnato alla colonna quando viene aggiornata una riga della tabella. Deve essere un valore appropriato al tipo di campo. Sono disponibili alcuni valori di parole chiave per determinati tipi di campo:

NOW

Specifica la data e l'ora correnti per una colonna di tipo DATE.

USER

Specifica l'utente attivo per una SREL della tabella Contatto.

Richiesto

Se selezionata, questa opzione indica che è necessario fornire un valore per la colonna prima di poter salvare una riga della tabella che la contiene. È possibile impostare questa opzione per le colonne standard e per le colonne definite a livello di sito. Inoltre è possibile disattivare un'opzione già impostata. Tuttavia, non è possibile disattivare l'opzione di una colonna standard a meno che non sia stata impostata in locale.

Aggiornabile solo per nuovo record

Se selezionata, questa opzione indica che è possibile specificare un valore per questa colonna solo dopo aver creato una riga della tabella relativa e non è possibile apportarvi successive modifiche. È possibile impostare questa opzione per le colonne standard e per le colonne definite a livello di sito. Inoltre è possibile disattivare un'opzione già impostata. Tuttavia, non è possibile disattivare l'opzione di una colonna standard a meno che non sia stata impostata in locale.

Tasto per pdm_userload

Se selezionata, questa opzione indica che la colonna è una tra quelle verificate da pdm_userload per determinare se il relativo input è un aggiornamento di una riga esistente. Questa opzione è disponibile solo per le colonne di tipo STRING. È un campo di sola lettura per tutte le colonne delle tabelle standard.

Opzioni di indice DBMS

Queste opzioni specificano le caratteristiche di una colonna che rappresenta un indice del DBMS fisico. Sono disponibili solo per le colonne delle tabelle definite in locale.

Univoco

Specifica che la colonna è univoca nella tabella e che due righe non possono avere lo stesso valore per la colonna.

Crescente

Specifica che l'indice del DBMS è elencato in ordine crescente in base a questa colonna. Questa opzione esclude l'opzione Decrescente.

Decrescente

Specifica che l'indice del DBMS è elencato in ordine decrescente in base a questa colonna. Questa opzione esclude l'opzione Crescente.

Schede Avanzate

Progettazione schema include una scheda Avanzate sia per le tabelle che per le colonne. Le informazioni in queste schede sono destinate all'assistenza tecnica e ai rappresentanti locali di CA. Poiché un amministratore o uno sviluppatore nella maggior parte dei casi non hanno necessità di usarle, queste schede non verranno trattate in questo documento.

Attività di Progettazione schema

Modifica di tabelle o colonne

Per modificare le informazioni su una tabella o colonna, selezionare la tabella o la colonna in Progettazione schema facendo clic su di essa, quindi specificare le nuove informazioni nei campi appropriati. Le informazioni che è possibile modificare dipendono dallo stato della tabella o della colonna:

- **Tabelle standard**—È possibile modificare i campi Nome visualizzato, Descrizione e Gruppo funzioni.

- **Colonne standard**—È possibile modificare i campi Nome visualizzato, Descrizione, Valore predefinito alla creazione e Valore impostato al salvataggio. Inoltre, è possibile selezionare le caselle di controllo Richiesto o Aggiornabile solo per nuovo record, nel caso non lo fossero. Se sono selezionate per impostazione predefinita, non è possibile deselezionarle. È comunque possibile annullare i cambiamenti.
- **Tabella definita dal sito**—Se la tabella non è pubblicata, è possibile modificare tutti i campi tranne Nome, che non può essere modificato dopo il salvataggio della nuova tabella. Dopo aver pubblicato una tabella definita a livello di sito, è possibile modificare solo i campi Nome visualizzato, Descrizione e Gruppo funzioni.
- **Colonna definita dal sito**—Se la colonna non è pubblicata, è possibile modificare tutti i campi tranne Nome, che non può essere modificato dopo il salvataggio della nuova colonna. Dopo che è stata pubblicata una colonna definita a livello di sito, è possibile modificare solo i campi Nome visualizzato, Descrizione, Valore predefinito alla creazione, Valore impostato al salvataggio e le caselle di controllo Richiesto e Aggiornabile solo per un nuovo record, Chiave per pdm_userload e le opzioni di indice del DBMS.

Aggiunta di una nuova tabella

Per aggiungere una nuova tabella al database

1. Scegliere Aggiungi tabella dal menu Modifica o fare clic sul pulsante Aggiungi tabella.
Viene visualizzata la finestra di dialogo Aggiungi nuova tabella.
2. Specificare il nome della tabella nel campo Nome nuova tabella e fare clic su OK. Il nome di una tabella definita a livello di sito deve iniziare con la lettera "z" per evitare conflitti con future tabelle standard.
Screen Painter Web verifica il nome e aggiunge una "z" all'inizio del nome della tabella se necessario.
3. Completare i campi nella scheda Informazioni tabella in modo appropriato.

Aggiunta di una nuova colonna

Per aggiungere una nuova colonna a una tabella

1. Selezionare la tabella a cui si desidera aggiungere la colonna (o selezionare una colonna qualsiasi fra quelle esistenti nella tabella) e scegliere Aggiungi colonna dal menu Modifica o fare clic sul pulsante Aggiungi colonna.

Viene visualizzata la finestra di dialogo Aggiungi nuova colonna.

2. Specificare il nome della colonna nel campo Nome nuova colonna e fare clic su OK. Il nome di una colonna definita a livello di sito e aggiunta a una tabella standard deve iniziare con la lettera "z" per evitare conflitti con future colonne standard.

Screen Painter Web verifica il nome e aggiunge una "z" all'inizio del nome della colonna se necessario.

3. Immettere in modo appropriato i dati necessari nei campi della scheda Informazioni colonna.

Salvataggio dei cambiamenti

Per salvare i cambiamenti al database mentre è ancora in corso la modifica di tabelle o colonne, scegliere Salva dal menu File o fare clic su Salva. Screen Painter Web memorizza i cambiamenti allo schema nel database nella tabella wspotbl (per le modifiche alle tabelle) o wspotcol (per le modifiche alle colonne).

Test dei cambiamenti allo schema

Per apportare cambiamenti allo schema in modalità test, selezionare Salva e imposta su modalità test, dal menu File di Progettazione schema. In questo modo le modifiche vengono salvate nel database e sul server viene creato un file che definisce le modifiche nel motore oggetti. Il file si chiama wspotest.mods ed è memorizzato nella sottodirectory site/mods/majic della directory di installazione CA Service Desk Manager.

Dopo aver creato il file wspotest.mods, Screen Painter Web riavvia il motore oggetti in modo che possa usare le nuove modifiche. Questa operazione può durare da alcuni secondi a un paio di minuti, in base alla complessità dello schema. In attesa che il motore oggetti venga riavviato, Screen Painter Web visualizza una finestra di dialogo e l'aggiorna una volta completati il riavvio e la sincronizzazione della memoria interna con il motore oggetti aggiornato. Al termine, Screen Painter Web visualizza un messaggio indicante che lo schema è stato inserito nella modalità test. Fare clic su OK nella finestra del messaggio per iniziare a usare il nuovo schema e creare e modificare i moduli Web che lo usano.

Il file `wsptest.mods` riguarda solo il motore oggetti definito dall'opzione `wsp_domsrvr`. Altri motori oggetti sullo stesso server non elaborano questo file che non viene distribuito ad altri server. Inoltre, le nuove tabelle e colonne in modalità test sono definite per il motore oggetti come oggetti locali. Ciò significa che il motore oggetti le riconosce e quindi ne permette l'uso sui moduli Web. Tuttavia, esse non esistono nel database e non riguardano gli altri utenti. Gli utenti di CA Service Desk Manager non utilizzano il motore oggetti Screen Painter Web, quindi non sono interessati dai cambiamenti allo schema di cui si sta eseguendo il test.

Annullamento delle modifiche allo schema

Se si cambia idea e si desidera annullare le modifiche apportate allo schema in modalità test, è possibile tornare alla versione pubblicata dello schema. Poiché l'annullamento dei cambiamenti può avere effetti sugli altri utenti, questa opzione è disponibile solo se l'installazione ha previsto le opzioni `wsp_domsrvr` e `wsp_webengine` per dedicare un motore oggetti e un motore Web a Screen Painter Web.

Per annullare le modifiche allo schema in modalità test, selezionare **Togli da modalità test**, nel menu **File**. Screen Painter Web elimina il file `wsptest.mods` e il motore oggetti Screen Painter Web riporta lo schema alla precedente versione pubblicata.

Dopo aver eliminato il file `wsptest.mods`, Screen Painter Web riavvia il motore oggetti in modo da rigenerare lo schema interno. Questa operazione può durare da alcuni secondi a un paio di minuti, in base alla complessità dello schema.

Una volta completato il riavvio del motore oggetti, lo schema attivo torna alla versione pubblicata. I moduli Web modificati in funzione del nuovo schema non vengono ripristinati automaticamente e potrebbero non funzionare con lo schema pubblicato.

Pubblicazione delle modifiche allo schema

Una volta completate le modifiche allo schema, è possibile metterle a disposizione di tutti gli utenti pubblicandole. La pubblicazione di uno schema modificato è un processo a due fasi:

1. Creazione o aggiornamento dei file che descrivono lo schema modificato per il motore oggetti e i programmi di utilità di CA Service Desk Manager. Screen Painter Web crea i file seguenti nel motore Web definito dall'opzione `wsp_webengine` (con impostazione predefinita `web:local`);

wsp.mods

Descrive tutti i cambiamenti allo schema gestiti da Screen Painter Web per il motore oggetti.

wsp_schema.sch

Descrive tutte le tabelle e le colonne gestite da Screen Painter Web.

wsp_index.sch

Descrive gli indici del DBMS per le tabelle gestite da Screen Painter Web.

wsp.altercol

Assegna il nome alle nuove colonne create da Screen Painter Web ma non ancora definite per il DBMS.

wsp.altertbl

Assegna il nome alle nuove tabelle create da Screen Painter Web ma non ancora definite per il DBMS. Inoltre, Screen Painter Web distribuisce il file `wsp.mods` a tutti i server di CA Service Desk Manager con un motore oggetti.

2. Modifica del DBMS fisico contenente le informazioni sul nuovo schema. Questa fase richiede l'interruzione dei servizi CA Service Desk Manager e l'esecuzione dello script `pdm_publish` sul server principale.

Importante il passaggio 2 ha un impatto significativo sugli altri utenti, quindi è necessario pianificare attentamente la pubblicazione delle modifiche dello schema. Si consiglia di usare gli ordini di cambiamento CA Service Desk Manager per pianificare e ottenere l'approvazione alla pubblicazione dello schema pianificato.

Per iniziare la pubblicazione dello schema, selezionare Salva e pubblica dal menu File. Questa operazione crea i file necessari sui server CA Service Desk Manager ma non li riavvia. Quindi, i nuovi file non hanno un impatto immediato. Tuttavia, una volta creati, i file verranno usati al successivo riavvio dei servizi di CA Service Desk Manager. È quindi necessario chiudere al più presto i servizi ed eseguire lo script `pdm_publish` sul server primario dopo la pubblicazione delle modifiche dello schema.

Dopo aver completato la pubblicazione dello schema con Screen Painter Web, non è possibile apportare ulteriori cambiamenti mediante Progettazione schema finché non viene eseguito lo script `pdm_publish`. Per eseguire lo script `pdm_publish`, interrompere i servizi CA Service Desk Manager e immettere il comando `pdm_publish` nel prompt dei comandi.

Il comando `pdm_publish` effettua le operazioni seguenti:

- Verifica che vi siano modifiche allo schema prodotte con Screen Painter Web da pubblicare controllando l'esistenza dei file richiesti nella directory `mods` del sito.
- Verifica che i servizi CA Service Desk Manager siano stati interrotti.

- Riunifica tutti i file dello schema, sia quelli gestiti che quelli non gestiti da Screen Painter Web, in un unico file principale chiamato `ddict.sch`.
- Invia i comandi SQL appropriati al DBMS per definire le nuove tabelle e colonne.
- Scrive una riga in un file registro, `wsp_schema.log`, dopo ogni definizione DBMS riuscita di una tabella o di una colonna. Oltre a documentare le modifiche apportate allo schema, il file registro serve anche come promemoria per il comando `pdm_publish` stesso per consentire al comando di stabilire quali tabelle e colonne create da Screen Painter Web sono già state definite per il DBMS. Pertanto questo file non deve essere né spostato né modificato.
- Crea un dizionario dei dati CA Service Desk Manager.

Questi passaggi normalmente durano un minuto. Al termine, è possibile riavviare i servizi CA Service Desk Manager e iniziare a usare lo schema modificato. Se sono stati creati o modificati moduli Web per l'uso del nuovo schema, avviare Screen Painter Web e pubblicare i nuovi moduli Web.

Migrazione da test a produzione

Uno degli obiettivi dell'ideazione di Screen Painter Web era rendere sicure le operazioni di sviluppo e test delle modifiche apportate allo schema in un database di produzione. Funzioni come la modalità test e processi server Screen Painter Web dedicati sono di supporto a questo obiettivo. Tuttavia molti utenti preferiscono sviluppare proprie modifiche allo schema in un sistema di test indipendente e quindi eseguirne la migrazione a un sistema di produzione separato una volta completate, secondo la procedura indicata di seguito:

1. Copiare il contenuto delle tabelle `wsptbl` e `wspcol` dal database di test al database di produzione. Per compiere questa operazione, si consiglia di usare le utilità `pdm_extract` e `pdm_userload` CA Service Desk Manager.
2. Utilizzare Screen Painter Web sul sistema di produzione per pubblicare lo schema. Dopodiché, lanciare lo script `pdm_publish`.

Nota: usando Screen Painter Web per la pubblicazione, si è certi che tutti gli aggiornamenti necessari vengano distribuiti a tutti i server di produzione.

Ulteriori informazioni:

[Pubblicazione delle modifiche allo schema](#) (a pagina 293)

Modifica o eliminazione delle colonne definite a livello di sito dopo la pubblicazione

Una volta pubblicate le modifiche allo schema definite a livello di sito, Screen Painter Web le considera come lo schema standard e limita la possibilità di modificarlo ulteriormente. Se si desidera, è possibile eliminare una colonna definita a livello di sito o cambiare la lunghezza di una colonna STRING definita in locale. Queste attività possono essere eseguite manualmente, aggiornando il DBMS e lo schema dall'esterno di Screen Painter Web e quindi eseguendo lo script `pdm_wspupd` per aggiornare la tabella `wspcol` del database per sincronizzare Screen Painter Web con i cambiamenti esterni. È possibile usare la procedura seguente:

1. Individuare la sottodirectory `site/mods` (UNIX) o `site\mods` (Windows) nella directory di installazione CA Service Desk Manager.
2. Usando un editor di testi standard, modificare il file `wsp_schema.sch` per eliminare le colonne definite a livello di sito che non servono più o modificare la lunghezza delle colonne STRING definite a livello di sito. Queste sono le uniche modifiche supportate da questa procedura.

Importante Se una delle opzioni di indice (ad esempio, `UNIQUE`) è stata specificata per una colonna da eliminare, utilizzare un editor di testo standard per modificare il file `wsp_index.sch` e rimuovere i riferimenti alla colonna. Se la colonna era l'unica colonna indicizzata della tabella, rimuovere tutti i riferimenti alla tabella da `wsp_index.sch`.

3. Usando un editor di testo standard, modificare il file `majic/wsp.mods` (UNIX) o `majic\wsp.mods` (Windows) apportando le stesse modifiche di `wsp_schema.sch`, cioè eliminare le colonne definite a livello di sito non desiderate o modificare la lunghezza delle colonne STRING definite a livello di sito.
4. Aprire una sessione con prompt dei comandi e immettere il comando:
`pdm_wspupd`

Lo script `pdm_wspupd` legge `wsp_schema.sch` e lo confronta con la tabella `wspcol` nel database, scrivendo le eventuali differenze su una riga nella console. L'output è simile a:

```
PDM_WSPUPD. Aggiornamento della tabella wspcol da wsp_schema.sch.
Lettura di wsp_schema.sch per informazioni su DBMS corrente...
Lettura della tabella wspcol per informazioni sullo schema WSP...
Lunghezza della colonna STRING zSalesOrg.description cambiata da 350 a 400
Impossibile trovare la colonna zSalesOrg.sym in wsp_schema.sch. Eliminazione della riga wspcol
pdm_wspupd ha individuato 1 colonne gestite da WSP da aggiornare e 1 da eliminare. Verificare che
DBMS sia stato aggiornato manualmente in modo che corrisponda a nwsp_schema.sch, quindi rispondere
S per aggiornare wspcol o qualsiasi altra cosa per annullare.
```


Verificare che le modifiche trovate da `pdm_wspupd` corrispondano esattamente a quelle apportate a `wsp_schema.sch`. In caso affermativo, digitare "S" per confermare le modifiche. Dopo aver confermato l'aggiornamento, lo script usa le utilità CA Service Desk Manager standard per aggiornare la tabella `wspcol`. In questo modo Progettazione schema di Screen Painter Web può visualizzare i cambiamenti.

5. Interrompere i servizi CA Service Desk Manager.
6. Usando l'utilità appropriata al DBMS, modificare la definizione DBMS delle colonne modificate. Eliminare dal database tutte le colonne eliminate da `wsp_schema.sch` e modificare nel database la lunghezza di tutte le colonne `STRING` modificate in `wsp_schema.sch`. Assicurarsi che le modifiche apportate al DBMS corrispondano esattamente alle modifiche apportate a `wsp_schema.sch`.
7. Eseguire `pdm_publish` come descritto precedentemente in Pubblicazione delle modifiche allo schema.
8. Avviare i servizi CA Service Desk Manager.

Personalizzazione dell'interfaccia Web

L'interfaccia Web CA Service Desk Manager (chiamata anche interfaccia del browser) fornisce la funzionalità CA Service Desk Manager tramite Internet, inclusa la possibilità di aprire, aggiornare o chiudere ticket, visualizzare e pubblicare annunci e accedere alle tabelle dei dati di supporto. Consente inoltre di consultare in modo autonomo la Knowledge Base e di ridurre il numero delle chiamate all'assistenza clienti e accelerare i tempi di risoluzione. L'interfaccia Web può essere completamente personalizzata e usata con i più diffusi browser Web.

Se è installata e configurata l'interfaccia Web, è possibile integrarla nella propria interfaccia Web esistente e personalizzarla ulteriormente per adattarla alle proprie esigenze. Per la personalizzazione, occorre conoscere il codice HTML e il browser Web in uso nella propria organizzazione.

Nota: la visualizzazione di progettazione di Screen Painter Web funziona per controlli CA Service Desk Manager (`PDM_MACROS`). Quando si lavora con moduli che non contengono controlli CA Service Desk Manager, è possibile usare solo la scheda Fonte. I moduli Web Dipendente e Cliente non contengono controlli CA Service Desk Manager, pertanto vengono visualizzati nella scheda Fonte anziché in Progetto. Alcuni moduli analista non contengono controlli CA Service Desk Manager, per cui comparirebbero anche nella scheda Sorgente.

Importante Il supporto tecnico non fornisce assistenza per la progettazione o il debugging delle personalizzazioni (né per la documentazione come i sistemi di Guida in linea). Vengono fornite informazioni generali per personalizzare l'interfaccia Web di CA Service Desk Manager. Durante questa operazione, tenere presente che si è gli unici responsabili delle proprie personalizzazioni. Il supporto tecnico di CA Service Desk Manager può aiutare ad interpretare e capire la personalizzazione.

Il supporto per le tecniche di personalizzazione qui descritte è esteso anche a garantire che le tecniche e gli strumenti funzionino correttamente. Non utilizzare funzioni non documentate e non sfruttare quelle documentate oltre le capacità descritte. Questi interventi non sono supportati e potrebbero causare problemi o instabilità al sistema che potrebbero apparire come non correlati alla personalizzazione. Per questo motivo, il supporto può chiedere di rimuovere le personalizzazioni per riprodurre i problemi. Per essere preparati a questa evenienza, seguire scrupolosamente le istruzioni su come inserire tutte le modifiche nella struttura di directory site/mods e gestire i registri dei cambiamenti. Chi apporta cambiamenti frequenti, complessi o estesi deve considerare la personalizzazione di CA Service Desk Manager come un progetto di software engineering e mantenere un rigoroso controllo del codice fonte, eseguire test e rilasciare release collaudate alla fase di produzione.

La migrazione di personalizzazioni tra le versioni può presentare problemi insoliti, per cui il prodotto è stato sviluppato in modo da salvaguardare gli sforzi impiegati nella personalizzazione. Tuttavia, si presuppone che il prodotto sia stato personalizzato secondo quanto documentato in questa guida, in particolare riguardo al posizionamento di tutte le personalizzazioni nella struttura mod del sito. Inoltre, nel caso in cui il supporto di secondo livello fornisca una patch per un sistema, la patch deve essere scritta con gli stessi presupposti. Applicare una patch o eseguire la migrazione di un sistema con personalizzazioni fuori controllo è un rischio che spesso comporta costosi fermi del sistema. Pertanto, evitare questo rischio seguendo questa guida e mettendo in pratica principi di software engineering.

Nota: per informazioni su come proteggere e configurare l'interfaccia Web, vedere la *Guida all'amministrazione*.

Il Screen Painter Web (WSP)

Lo strumento principale per la personalizzazione di CA Service Desk Manager è Screen Painter Web. Questo strumento può essere installato in qualsiasi server CA Service Desk Manager. Fornisce un'interfaccia utente semplice e intuitiva che consente di personalizzare i moduli Web e gli schemi secondo le proprie esigenze senza ricorrere alla programmazione. Screen Painter Web può essere usato per eseguire molte attività tra cui:

- Cambiamento delle etichette dei campi.
- Spostamento dei campi in un modulo o cambiamento dell'aspetto di un elenco.
- Aggiunta di campi a un modulo o di colonne a un elenco.
- Aggiunta di un notebook a un modulo o cambiamento delle schede in un notebook esistente.
- Creazione di moduli e di gruppi di moduli.
- Personalizzazione dei file CSS (Cascading Style Sheet).
- Visualizzazione in anteprima dei cambiamenti in una finestra del browser prima della pubblicazione per gli altri utenti.
- Aggiunta di nuove tabelle o colonne al database o cambiamento delle caratteristiche delle colonne esistenti.
- Visualizzazione in anteprima dei moduli che utilizzano schemi personalizzati prima di cambiare il database.

È possibile eseguire tutte queste attività con semplici operazioni di trascinamento della selezione o di puntamento e doppio clic sul controllo che interessa nella Casella dei controlli, senza dover ricorrere alla programmazione o intervenire sul codice sorgente del modulo. Comunque, se si desidera esaminare e modificare il codice fonte, Screen Painter Web fornisce anche un editor del codice fonte che evidenzia le parole chiave e integra perfettamente i cambiamenti al livello di codice con quelle alla vista di progettazione.

Tuttavia, alcuni dei moduli di Gestione delle informazioni non possono essere personalizzati nella vista di progettazione di Screen Painter Web. Per la personalizzazione di questi moduli sono previsti approcci alternativi, ad esempio i seguenti:

- Visualizzazione documento - Il contenuto di questa pagina è determinato dal modello utilizzato per la creazione del documento. Questi modelli possono essere modificati nella scheda Amministrazione, in Documenti, Modelli documento.
- Elenco documenti categorie della conoscenza - È possibile modificare questa pagina utilizzando Screen Painter Web, ma anche mediante le preferenze utente. La schermata "Preferenze" fornisce opzioni di personalizzazione per l'utente finale che consentono di definire quali proprietà del documento visualizzare nell'elenco dei documenti e quanti documenti visualizzare per pagina.

Nota: per la modifica dello schema mediante l'aggiunta di nuove tabelle e colonne è richiesta l'autorizzazione dell'amministratore.

Ulteriori informazioni:

[Personalizzazione dello schema](#) (a pagina 282)

Avvio di Screen Painter Web (Windows)

È possibile avviare Screen Painter Web in qualsiasi momento per personalizzare, senza programmazione, moduli Web e lo schema in base alle proprie esigenze. Per avviare Screen Painter Web, scegliere Start, Programmi, CA, Service Desk, Screen Painter Web. Viene visualizzato un modulo di accesso standard di CA Service Desk Manager in un browser. Una volta effettuato l'accesso, Screen Painter Web visualizza il modulo principale.

Avvio di Screen Painter Web (UNIX)

È possibile avviare Screen Painter Web in qualsiasi momento per personalizzare, senza programmazione, moduli Web e lo schema in base alle proprie esigenze. Per avviare Screen Painter Web, introdurre il comando *pdm_wsp* con *\$NX_ROOT/bin* nel percorso. Una volta effettuato l'accesso, Screen Painter Web visualizza il modulo principale.

Nota: quando si usa UNIX, occorre avere Firefox installato per utilizzare Screen Painter Web.

Apertura di un modulo per la modifica

È possibile aprire un modulo in Screen Painter Web per modificare il contenuto e l'aspetto delle informazioni del modulo.

Per aprire un modulo per la modifica

1. Selezionare File, Open.

Viene visualizzata la finestra di dialogo Apri modulo.

2. Selezionare l'interfaccia (Analista, Cliente, Dipendente, Predefinito) o il tipo di file (fogli di stile CSS, JavaScript o HTML) e il gruppo di moduli contenente quello da modificare.
3. Selezionare il modulo dall'elenco a scorrimento o immettere il nome nella casella di testo.

Quando si immette un nome nella casella di testo, Screen Painter Web scorre automaticamente l'elenco fino a trovare il primo nome che corrisponde ai caratteri immessi.

Per limitare il numero di file visualizzati, è possibile usare l'elenco a discesa File di stato:

Sito modificato con modifiche non pubblicate (+)

Limita l'elenco ai file che sono stati modificati con Screen Painter Web ma che non sono ancora stati pubblicati. Questi file sono identificati da un segno più (+) posto dopo il nome file.

Sito modificato (*)

Limita l'elenco ai moduli modificati in locale, sia quelli pubblicati che quelli non pubblicati. I file non pubblicati sono identificati da un segno più (+) posto dopo il nome file; quelli con modifiche in locale pubblicate sono identificati da un asterisco (*) posto dopo il nome file.

Tutti

Mostra tutto l'elenco senza restrizioni. I file non pubblicati sono identificati da un segno più (+) posto dopo il nome file; quelli con modifiche in locale pubblicate sono identificati da un asterisco (*) posto dopo il nome file.

Importante Quando si crea o modifica un modulo dettaglio o elenco, assicurarsi di utilizzare i prefissi "list_" e "detail_" per denominare il file HTML. Ad esempio, utilizzare "list_test.html" e "detail_test.html". L'aggiunta di questo prefisso consente di visualizzare correttamente in anteprima un modulo. Quando si salva un modello di dettaglio con un nome personalizzato, è anche necessario modificare manualmente il tag <PDM_WSP>. Ad esempio, <PDM_WSP mode=edit preview="test.html+OP=CREATE_NEW" factory=cr>.

Creazione di un modulo

È possibile creare un modulo utilizzando Screen Painter Web.

Per creare un modulo

1. Selezionare File, Nuovo.
Viene visualizzata la finestra di dialogo Nuovo modulo.
2. Selezionare un'interfaccia, un gruppo di moduli e il tipo di modulo (dettagli, elenco o barra dei menu).
3. Selezionare un factory (o tabella) per il nuovo modulo.

Nota: in un gruppo di moduli può esserci un solo modulo dettagli o elenco per tabella, pertanto, per quelle tabelle che già dispongono di un modulo, è necessario modificare il modulo esistente anziché crearne uno nuovo. Se si desidera disporre di più versioni di un modulo, creare uno o più gruppi di moduli per conservare le varie versioni.

Importante Quando si crea o si modifica un modulo dettaglio o elenco, utilizzare i prefissi "list_" e "detail_" per denominare il file HTML. Ad esempio, utilizzare "list_test.html" e "detail_test.html". L'aggiunta di questo prefisso consente di visualizzare correttamente in anteprima un modulo. Quando si salva un modello di dettaglio con un nome personalizzato, è inoltre necessario modificare manualmente il tag <PDM_WSP>. Ad esempio, <PDM_WSP mode=edit preview="test.html+OP=CREATE_NEW" factory=cr>.

Ulteriori informazioni:

[Modalità di creazione di un gruppo di moduli Web](#) (a pagina 320)

Finestra di modifica del modulo

Dopo aver aperto un modulo esistente, o viene richiesto di crearne uno, compare la finestra Modifica modulo. In questa finestra sono presenti due schede, Progetto e Origine. La scheda Progetto è disponibile per i moduli dettagli, elenco e barra dei menu. In questa scheda la disposizione dei controlli è simile a quella visualizzata dall'utente finale. Non è un'immagine di come l'utente finale visualizza il modulo. Per visualizzarla, selezionare Strumenti, Anteprima.

La scheda Progetto è un editor simile a Blocco note e consente di esaminare e modificare il codice sorgente di un modulo. Alcuni moduli possono essere modificati solo nella scheda Progetto. Per questi moduli, la finestra di modifica si apre direttamente nella scheda Progetto; la scheda Progetto è disattivata.

La barra del titolo della finestra di modifica mostra il nome del modulo, l'interfaccia e il gruppo di appartenenza, se appropriato. È possibile aprire finestre di modifica per più di un modulo contemporaneamente.

Importante Quando si crea o modifica un modulo dettaglio o elenco, assicurarsi di utilizzare i prefissi "list_" e "detail_" per denominare il file HTML. Ad esempio, utilizzare "list_test.html" e "detail_test.html". L'aggiunta di questo prefisso consente di visualizzare correttamente in anteprima un modulo. Quando si salva un modello di dettaglio con un nome personalizzato, è anche necessario modificare manualmente il tag <PDM_WSP>. Ad esempio, <PDM_WSP mode=edit preview="test.html+OP=CREATE_NEW" factory=cr>.

Modifica di moduli elenco e dettagli nella vista Progetto

La scheda vista Progetto mostra i controlli su un modulo, disposti nello stesso formato tabellare in cui verrebbero visualizzati da un client. È possibile spostare questi controlli selezionandoli e trascinandoli in nuove posizioni. Per eliminare un controllo, fare click sul controllo e selezionare Modifica, Elimina.

La vista Progetto è usata per modificare i controlli. Non mostra il modulo come verrebbe visualizzato da un utente finale. Per visualizzare il modulo come appare a un utente finale, selezionare Strumenti, Anteprima. Le differenze principali tra la vista Progetto e la vista dell'utente finale sono:

- Nella vista Progetto non sono usati caratteri e stili.
- Ogni controllo mostra il nome dell'attributo associato nella vista Progetto.
- Screen Painter Web mostra solo i controlli CA Service Desk Manager (quelli definiti dalle istruzioni <PDM_MACRO>). Non mostra il contenuto definito dai tag standard HTML o JavaScript.
- Screen Painter Web mostra tutti i controlli sul modulo, indipendentemente dalle espressioni condizionali (istruzioni PDM_IF). Ciò consente di modificare tutti gli elementi presenti in un modulo. Screen Painter Web mostra i controlli condizionali come testo in rosso, ad esempio If o Else.

Finestra di dialogo Proprietà

Per modificare le proprietà di un controllo (compresa l'etichetta), aprire la finestra di dialogo Proprietà facendo click sul controllo nel modulo e selezionando Controlli, Proprietà. Tutte le finestre di dialogo Proprietà contengono i campi nome Attributo (colonna), Didascalia (etichetta) e Ampiezza colonna (il numero di colonne nella griglia). Gli altri campi nella finestra di dialogo Proprietà cambiano a seconda del tipo di controllo.

Per cambiare un valore in una finestra di dialogo Proprietà, digitare il nuovo valore nello spazio apposito. Le modifiche diventano effettive non appena si fa clic all'esterno del campo o si chiude la finestra di dialogo.

Screen Painter Web visualizza un breve riepilogo del significato di una proprietà in una nota che appare nella parte inferiore del modulo Proprietà quando si seleziona la proprietà.

Inserimento di un controllo

È possibile inserire un controllo in un modulo nei modi seguenti:

- Selezionare e trascinare il controllo dalla Casella dei controlli, nella parte sinistra della finestra principale di Screen Painter Web, nella posizione desiderata sul modulo.
- Fare clic su una posizione sul modulo in cui si desidera inserire il nuovo controllo e selezionare il controllo dal menu Controllo.
- Copiare un controllo esistente e incollarlo sul modulo.

Dopo che il nuovo controllo è stato posizionato correttamente, visualizzarne e modificarne le proprietà.

Di seguito sono indicati i controlli che possono essere inseriti sia nei moduli dettagli che in quelli elenco sono:

Controllo	Icona	Descrizione
Inserisci Riga		Determina lo spostamento del controllo selezionato nell'ultima posizione della riga corrente e sposta i controlli successivi nella nuova riga.
Elimina Riga	N/D	Elimina tutti i controlli presenti sulla stessa riga del controllo selezionato.
Casella di testo		Inserisce una casella di testo a una riga o a più righe per modificare un campo di tipo stringa o testo.
Elenco a discesa		Inserisce un elenco a discesa per la modifica di un campo convalidato rispetto ad una tabella.
Ricerca		Inserisce un controllo di tipo ricerca per modificare un campo convalidato rispetto a una tabella. Il controllo è composto da una casella di testo la cui etichetta presenta un collegamento ipertestuale che apre un determinato modulo.
Pulsante		Inserisce un pulsante.

Controllo	Icona	Descrizione
Ricerca gerarchica		Simile al controllo Ricerca tranne per il fatto che è usato per un campo con un selettore gerarchico (ad esempio la categoria della richiesta).
Data		Inserisce un campo per la data. Il controllo è composto da una casella di testo la cui etichetta presenta un collegamento ipertestuale che apre un selettore di date.

I controlli seguenti sono disponibili solo per i moduli dettagli:

Controllo	Icona	Descrizione
Casella di controllo		Inserisce una casella di controllo.
Editor HTML		Inserisce un editor HTML per un campo di testo contenente codice HTML.
Casella di testo sola lettura		Inserisce un campo di testo non-modificabile.
Ricerca sola lettura		Inserisce un campo di ricerca non-modificabile. Il campo viene visualizzato come collegamento ipertestuale che apre il modulo dettagli che lo definisce.
Sola lettura		Inserisce un campo per la data non-modificabile.
Notebook		Inserisce un notebook. In un modulo dettagli può esserci solo un notebook, pertanto questo controllo può essere inserito solo sui moduli che non contengono già un notebook.

Il controllo seguente è disponibile solo per i moduli elenco:

Controllo	Icona	Descrizione
Elenco		Inserisce un elenco. In un modulo elenco può esserci solo un elenco, pertanto questo controllo può essere inserito solo su nuovi moduli elenco.

Progettazione notebook

Molti moduli dettagli contengono un notebook con due o più schede. È possibile utilizzare il controllo Notebook per aggiungere un notebook ad un modulo dettagli che non ne contiene ancora nessuno. La finestra di dialogo Proprietà per un controllo Notebook è sostituita da Progettazione notebook. Per aprire Progettazione notebook, fare doppio clic sul controllo Notebook.

Progettazione notebook consente di aggiungere, inserire ed eliminare schede e modificarne le didascalie. Inoltre, è possibile utilizzare i pulsanti freccia verso l'alto e verso il basso per cambiare la disposizione delle schede cambiando la posizione della scheda correntemente selezionata. La casella di controllo Nuova riga specifica se la scheda selezionata deve iniziare o meno con una riga nuova nell'intestazione del notebook.

CA Service Desk Manager supporta due tipi di schede del notebook:

- Una *scheda rinviata* viene caricata solo se selezionata dall'utente nell'intestazione del notebook. La voce relativa in Progettazione notebook specifica un URL. Questo URL può essere un URL Web standard (che inizia per http://) o un URL CA Service Desk Manager (che inizia per OP=). Per specificare una scheda rinviata, selezionare la casella di controllo Rinvia.
- Una *scheda standard* viene caricata insieme al modulo. La voce relativa in Progettazione notebook specifica il nome di un file HTML che definisce il contenuto della scheda, che deve essere racchiuso tra i tag <pdm_form> nel file. Per specificare una scheda standard, deselezionare la casella di controllo Rinvia.

Il contenuto di una scheda standard è definito in un file HTML separato. Per modificare questo file con Screen Painter Web, fare doppio clic sul nome file del collegamento ipertestuale mostrato da Screen Painter Web nel corpo della scheda nella vista Progetto. Il file HTML che definisce la scheda viene aperto in un'altra finestra di modifica del modulo.

Progettazione elenco

I moduli elenco di CA Service Desk Manager sono generalmente costituiti da un filtro di ricerca nella parte superiore e da un elenco in quella inferiore. La sezione del filtro di ricerca di un modulo elenco è simile a un modulo dettagli ed è modificabile allo stesso modo. L'unica differenza è che in questa finestra sono disponibili meno controlli. I moduli elenco supportano solo i controlli casella di testo, elenco a discesa, data, ricerca, pulsante di comando e ricerca gerarchica.

In Screen Painter Web è visualizzata la sezione dell'elenco come un riquadro rettangolare vuoto con le intestazioni nella parte superiore. La finestra di dialogo Proprietà per un controllo Elenco è sostituita da Progettazione elenco. Per visualizzare Progettazione elenco, fare doppio clic sul controllo Elenco.

Progettazione elenco consente di aggiungere, inserire ed eliminare attributi e di modificarne le didascalie (intestazioni delle colonne). Inoltre, è possibile utilizzare i pulsanti freccia verso l'alto e verso il basso per cambiare la disposizione degli attributi modificando la posizione dell'attributo correntemente selezionato. La casella di controllo Nuova riga specifica se l'attributo selezionato inizia una nuova riga di attributi nei dati per una singola riga del database.

Nota: per ulteriori informazioni sugli altri campi di questo modulo, consultare la *Guida di Screen Painter Web*.

Controlli condizionali

CA Service Desk Manager supporta l'inserimento di contenuto in un modulo a determinate condizioni. Ad esempio, il modulo Dettagli richiesta (detail_cr.html) usa un controllo di ricerca per l'attributo change solo per le nuove richieste. Per le richieste esistenti, utilizza una ricerca in sola lettura che viene visualizzata nella vista Progettazione.

In Screen Painter Web sono visualizzati entrambi i controlli della casella di testo per l'attributo change, tuttavia l'utente finale ne visualizza solo uno alla volta. Il controllo condizionale viene mostrato in rosso, ad esempio If o Else. È possibile visualizzare la finestra di dialogo Proprietà di un controllo condizionale con la stessa procedura utilizzata per un controllo normale.

I controlli condizionali mostrati da Screen Painter Web corrispondono a PDM_IF e ai tag associati. PDM_IF: l'elaborazione condizionale descrive questi tag e la sintassi di un controllo condizionale.

Screen Painter Web mostra quattro tipi di controlli condizionali:

Controllo	Icona	Descrizione
If		Inizia un'espressione condizionale.
Elif		(Facoltativo) Specifica una condizione alternativa (else if). È possibile usare un numero qualsiasi di controlli elif.
Else		(Facoltativo) Specifica un'alternativa. Se usato, deve essere l'ultimo controllo prima di endif.
Endif		(Obbligatorio) Termina l'espressione condizionale.

Anteprima moduli

Per vedere come verrà visualizzato un modulo all'utente finale, selezionare Strumenti, Anteprima. In Screen Painter Web il modulo modificato viene copiato sul server e memorizzato in una directory accessibile solo per le richieste di anteprima di Screen Painter Web, quindi viene inviato un URL per consentire l'apertura del modulo in una finestra del browser.

In una finestra di anteprima di Screen Painter Web è possibile visualizzare un modulo così come viene visualizzato ad un utente finale. Sebbene sia simile a una finestra CA Service Desk Manager standard e presenti numerosi pulsanti e menu funzionanti, la finestra di anteprima non è una sessione standard e non deve essere utilizzata come tale. Di seguito sono riportate le principali limitazioni di una sessione di anteprima:

- Normalmente la finestra è di sola lettura. Ciò significa che, sebbene sia possibile utilizzare funzioni come la modifica dei dati, tutte le richieste di aggiornamento del database vengono ignorate. Non è infatti possibile cambiare il database in una sessione di anteprima di Screen Painter Web. La finestra del browser indica questa limitazione in due modi:
 - L'icona rossa di Screen Painter Web nell'angolo superiore sinistro indica che la finestra del browser mostra una sessione di anteprima di sola lettura. L'amministratore CA Service Desk Manager può consentire gli aggiornamenti nella finestra di anteprima, Tuttavia si consiglia di evitarlo. Se l'amministratore ha configurato Screen Painter Web in questo modo, l'icona è gialla (attenzione).
 - Ogni ricorrenza della parola "Salva" su un pulsante o un menu viene sostituita da un'indicazione che ne comunica l'impossibilità di eseguire il salvataggio e di aggiornare il database.
- Non tutte le funzioni sono disponibili. L'anteprima di Screen Painter Web visualizza sempre il modulo o la scheda su cui si sta lavorando. Tuttavia, molti moduli sono concepiti per essere selezionati tramite uno specifico percorso dell'applicazione e l'ambiente potrebbe non essere configurato correttamente quando vengono visualizzati direttamente. Se si fa clic su un pulsante o si tenta di usare una funzione non impostata in modo appropriato, viene visualizzato un messaggio che indica che la funzione non è disponibile in modalità di anteprima.
- In Screen Painter Web viene sempre visualizzato un modulo dettagli nella vista di modifica che viene compilato con i dati del database utilizzando le righe aggiunte di recente della tabella appropriata che si è autorizzati a visualizzare. Per esaminare la vista di sola lettura del modulo, fare clic sul pulsante noSave.

- Viene sempre visualizzato un modulo elenco che riporta una singola riga del database, con il relativo filtro di ricerca chiuso. È possibile visualizzare e modificare il filtro di ricerca e ripetere la ricerca per visualizzare l'anteprima del modulo.

Per impostazione predefinita, nell'anteprima di Screen Painter Web viene visualizzato un modulo dettagli nella vista di modifica o un modulo elenco nella vista di elenco. È possibile modificare questa impostazione per un particolare modulo HTML con il tag PDM_WSP, come descritto in PDM_WSP: controllo dell'anteprima Web Screen Painter.

Modifica nella vista Origine

Talvolta è necessario intervenire sul codice sorgente di un modulo, ad esempio per la modifica di moduli diversi dai moduli elenco o dettagli o per la modifica di elementi dei moduli HTML o JavaScript che non sono mostrati nella vista Progetto. Per passare alla vista Fonte di un modulo, fare clic sulla scheda Fonte per visualizzare il codice sorgente del modulo.

Se è selezionato un controllo, Screen Painter Web sposta automaticamente il cursore all'inizio del codice sorgente che definisce il controllo.

L'editor della vista Origine è un normale editor di testi, simile al Blocco note di Windows, tranne per il fatto che la vista Origine è codificata a colori. Le parole chiave, ad esempio HTML, sono evidenziate e colorate. È possibile controllare il carattere e il colore del codice usati nella vista Origine scegliendo Opzioni dal menu Strumenti. La finestra di dialogo Opzioni mostra il carattere usato nella vista Origine e il colore predefinito per otto elementi HTML e JavaScript. Per cambiare un colore, fare clic sul pulsante con i puntini di sospensione accanto ad esso e selezionare il colore desiderato nella tavolozza.

Modifica delle barre dei menu

I moduli i cui nomi iniziano con *"menubar_"* definiscono una barra dei menu. Nella vista Progetto di una barra dei menu il menu è visualizzato nella parte superiore. Nella vista Progetto non è possibile modificare direttamente la barra dei menu, ma solo fare clic su una voce di menu per aprirlo. Per modificare una barra dei menu, fare doppio clic sulla voce di menu per visualizzare Progettazione menu.

Nota: i menu e i moduli barra dei menu vengono usati solo nell'interfaccia dell'analista. Nelle interfacce di cliente e dipendente viene utilizzata una barra di avvio contenente i collegamenti veri e propri e non gli elenchi a discesa. Per personalizzare la barra di avvio per l'interfaccia Cliente o Dipendente, modificare il modulo `std_body_site.html` dall'interfaccia appropriata.

Progettazione menu consente di aggiungere, inserire ed eliminare menu e voci di menu e di modificarne le didascalie. È possibile utilizzare i pulsanti freccia verso l'alto e verso il basso per cambiare la disposizione dei menu e degli elementi cambiando la posizione dell'elemento selezionato.

I pulsanti Aggiungi e Inserisci comportano l'inserimento di una nuova voce di menu. Se si utilizza Aggiungi, la nuova voce di menu viene inserita alla fine del menu, se si utilizza Inserisci viene posizionata prima della voce correntemente selezionata.

Per inserire una nuova voce sulla barra dei menu

1. Aggiungere o inserire una voce di menu.
2. Fare clic sul pulsante freccia sinistra per convertirla in una voce della barra dei menu.
3. Fare clic sul pulsante freccia destra se si desidera annullare l'operazione.

Nota: per informazioni sui campi del modulo, vedere la *Guida in linea di Screen Painter Web*.

Funzioni utili nelle voci di menu

CA Service Desk Manager fornisce una barra dei menu in quasi tutti i moduli per controllarne le funzioni. La barra di menù viene generata da un modulo HTML con il nome del modulo `menubar_xx.html`. Si raccomanda di utilizzare Screen Painter Web per personalizzare le barre di menù esistenti e per crearne di nuove.

Le funzioni predefinite seguenti possono essere utili per gli script richiamati dalle voci dei menu:

upd_frame(modulo)

Carica un nuovo modulo nel frame del contenuto della finestra principale.

create_new(factory, use_template, width, height [,args])

Visualizza un modulo per definire un nuovo record.

`Popup_window(name, form[, width, height [,features [,args]]])`

Visualizza una nuova finestra.

showDetailWithPersid(persid)

Visualizza un record dettagli.

Ecco la spiegazione dei termini e delle definizioni validi per le funzioni precedenti:

modulo

Rappresenta il nome del file HTML, nel formato xxx.html, o il codice di un'operazione, ad esempio CREATE_NEW.

factory

Rappresenta il nome dell'oggetto del database.

usa_modello

Può essere True o False.

larghezza

Rappresenta la larghezza desiderata del modulo; il valore predefinito è zero.

altezza

Rappresenta l'altezza desiderata del modulo; il valore predefinito è zero.

caratteristiche

Rappresenta un elenco di funzioni della finestra nello stesso formato utilizzato con la funzione window.open standard.

argomenti

Rappresenta uno o più argomenti di tipo "parola chiave=valore" per l'operazione specificata per il modulo.

persid

Rappresenta l'ID persistente di tipo factory:id.

Modifica dei fogli di stile

È possibile utilizzare Screen Painter Web per modificare o creare i file CSS (Cascading Style Sheet).

Per modificare un foglio di stile

1. Selezionare File, Open.

Viene visualizzata la finestra di dialogo Apri modulo.

2. Selezionare Foglio di stile CSS dall'elenco a discesa Tipo interfaccia o tipo file.

Viene visualizzato un elenco di fogli di stile.

Per creare un foglio di stile

1. Selezionare File, Nuovo.

Viene visualizzata la finestra di dialogo Nuovo modulo.

2. Selezionare Foglio di stile CSS dall'elenco a discesa Tipo interfaccia o tipo file e fare clic su Nuovo.

In entrambi i casi, Screen Painter Web visualizza la vista Fonte del foglio di stile. È possibile modificare il foglio direttamente nella vista Fonte oppure visualizzare Progettazione stile selezionando Strumenti, Progettazione stile.

La sezione superiore di Progettazione stile consente di controllare le classi all'interno del foglio di stile. L'elenco a discesa Classi stili, nella parte superiore sinistra di Progettazione stile, consente di selezionare una classe da modificare. I pulsanti Aggiungi, Rinomina ed Elimina consentono di creare una nuova classe oppure di rinominare o eliminare una classe esistente.

In Progettazione stile sono presenti tre schede. La scheda Carattere e colore consente di selezionare gli attributi per la formattazione del testo per mezzo della classe dello stile e di visualizzare in anteprima il risultato finale. La sezione Anteprima carattere di questa scheda mostra come apparirà lo stile.

La scheda Posizione consente di controllare la collocazione e la scheda Altro di controllare gli attributi di visibilità, visualizzazione, overflow e cursore. Esistono numerosi attributi di stile, come il margine e il bordo, che non possono essere né visualizzati né modificati in Progettazione stile. Devono essere modificati nella vista Origine.

Quando si fa clic su OK in Progettazione stile, Screen Painter Web riformatta il foglio di stile e aggiorna la vista Fonte. È possibile continuare ad apportare modifiche nella vista Origine o aprendo di nuovo Progettazione stile.

Nota: per motivi di prestazioni, alcuni fogli di stile di CA Service Desk Manager sono disponibili in due formati: file singoli (ad esempio search_filter.css) e file di combinazione che raggruppano un determinato numero di file singoli con commenti e spazio in eccesso rimosso (ad esempio analyst_styles.css). Screen Painter Web modifica sempre i file individuali; non è possibile modificare direttamente una combinazione di file. Quando si pubblicano i cambiamenti ai fogli di stile, Screen Painter Web genera automaticamente il file di combinazione associato, se necessario.

Modifica dei moduli HTML e JavaScript

È possibile usare la vista Fonte di Screen Painter Web per modificare i moduli HTML e JavaScript. Per modificare entrambi, selezionare File, Apri. Viene visualizzata la finestra di dialogo di apertura del file di Screen Painter Web. Selezionare HTML o JavaScript dall'elenco a discesa Tipo interfaccia o tipo file per visualizzare l'elenco dei file disponibili per la modifica.

Nota: per motivi di prestazioni, alcuni file JavaScript di CA Service Desk Manager sono disponibili in due formati: file singoli (ad esempio `window_manager.js`) e file di combinazione che raggruppano un determinato numero di file singoli con commenti e spazio in eccesso rimosso (ad esempio `std_head.js`). In Screen Painter Web vengono modificati sempre i file singoli. Non è possibile modificare direttamente una combinazione di file. Quando si pubblicano i cambiamenti agli script, Screen Painter Web genera automaticamente il file di combinazione associato, se necessario.

Salvataggio delle modifiche

Le modifiche apportate possono essere salvate in qualsiasi momento. Per salvare i cambiamenti a un file in particolare, selezionarne la finestra di modifica, quindi scegliere File, Salva. Per salvare i cambiamenti a tutti i file modificati, selezionare File, Salva tutto.

Note: Screen Painter Web salva sempre i cambiamenti sul server e non sul PC locale, a meno che questo non sia il server. Quando si salva un file, il file diventa accessibile agli altri utenti di Screen Painter Web in una sessione di anteprima ma resta invisibile agli utenti di CA Service Desk Manager. Questo accade perché Screen Painter Web salva tutti i file nella directory `site/mods/wsp` (UNIX) o `site\mods\wsp` (Windows) e questa directory non è usata da una normale sessione CA Service Desk Manager.

Eliminazione delle modifiche prima della pubblicazione

Se non si è soddisfatti dei cambiamenti apportati, è possibile eliminarli prima della pubblicazione. L'eliminazione dei cambiamenti comporta l'eliminazione di un nuovo modulo oppure la conferma dello stato corrente di un modulo esistente.

Per eliminare i cambiamenti, selezionare File, Elimina modulo.

Le richieste di eliminazione dei moduli hanno effetto al momento di pubblicare i cambiamenti.

È possibile annullare una richiesta di eliminazione in sospeso scegliendo Annulla eliminazione modulo dal menu File.

La richiesta di eliminazione viene annullata. Non è possibile annullare i cambiamenti dopo la pubblicazione; l'unico modo per cambiare un modulo pubblicato è modificarlo nuovamente.

Eliminazione dei moduli dopo la pubblicazione

È possibile eliminare solo i moduli modificati in locale. Le richieste di eliminazione di moduli già pubblicati vengono eseguite quando si pubblicano i cambiamenti.

Per annullare una richiesta di eliminazione in sospeso, selezionare File, Annulla eliminazione modulo.

I cambiamenti vengono annullati dopo la pubblicazione; l'unico modo per cambiare un modulo pubblicato consiste nel modificarlo nuovamente.

Pubblicazione delle modifiche

Una volta completate i cambiamenti dello schema, è possibile metterli a disposizione di tutti gli utenti CA Service Desk Manager pubblicandoli. La pubblicazione aggiorna tutti i server CA Service Desk Manager con i moduli nuovi o revisionati.

Per pubblicare i cambiamenti

1. Scegliere File, Pubblica.

In presenza di cambiamenti non salvati, Screen Painter Web chiede se si desidera salvarli, quindi visualizza una finestra di dialogo di conferma che mostra tutte i cambiamenti Screen Painter Web in sospeso (compresi quelli salvati in sessioni precedenti o salvati da altri utenti Screen Painter Web). Per impostazione predefinita, tutti i cambiamenti vengono selezionati per la pubblicazione. È possibile cambiare la selezione dei cambiamenti da pubblicare facendo clic su di essi.

2. Completata la selezione, fare clic su OK.

Screen Painter Web mette a disposizione di tutti gli altri utenti i cambiamenti selezionati.

Migrazione da test a produzione

Uno degli obiettivi dell'ideazione di Screen Painter Web era rendere sicure le operazioni di sviluppo e test delle modifiche apportate ai moduli in un database di produzione. Caratteristiche come una struttura di directory destinata esclusivamente a Screen Painter Web-sul server, processi server Screen Painter Web dedicati e sessioni di anteprima di sola-lettura sono di supporto a questo obiettivo. Tuttavia molti utenti preferiscono sviluppare modifiche personalizzate ai moduli in un sistema di test indipendente e quindi eseguirne la migrazione in un sistema di produzione separato una volta completate:

1. Copiare i moduli HTML di cui eseguire la migrazione dalla sottodirectory appropriata di site/mods/www/html nel sistema di test alla stessa sottodirectory di site/mods/wsp/project nel server principale del sistema di produzione.
2. Copiare i file CSS, JavaScript e HTML di cui eseguire la migrazione dalla sottodirectory appropriata di site/mods/www/wwwroot nel sistema di test alla stessa sottodirectory di site/mods/www/wwwroot/wsp/project nel server principale del sistema di produzione.

3. Utilizzare Screen Painter Web nel sistema di produzione per pubblicare i moduli. L'uso di Screen Painter Web per la pubblicazione garantisce che i moduli nuovi o aggiornati vengano distribuiti in tutti i server di produzione.

Per eseguire le operazioni di copia descritte nei passaggi 1 e 2 precedenti, è possibile usare qualsiasi metodo di copia dei file supportato dal sistema operativo. Gli utenti di Windows devono sostituire con la barra rovesciata (\) la barra (/) nei percorsi delle directory indicati.

Modelli HTML (moduli HTMPL)

I moduli nell'interfaccia Web di CA Service Desk Manager saranno distribuiti come modelli HTML, in file con estensione .htmpl. Questi sono chiamati moduli HTMPL nel resto di questo documento.

Un modulo HTMPL contiene codice HTML standard (compreso il codice JavaScript) oltre a estensioni del linguaggio che sono interpretate da un daemon (servizio) server CA Service Desk Manager, chiamato motore Web, che passa il codice HTML standard al browser. Queste estensioni sono:

- Riferimenti a variabili del server. Sono indicati da un nome che inizia con il simbolo del dollaro. Possono essere i valori delle colonne nel database CA Service Desk Manager, riferimenti alle proprietà di configurazione del motore Web o altre informazioni sul server.
- Tag speciali che indicano al motore Web di eseguire attività sul server, ad esempio di leggere le informazioni contenute nel database CA Service Desk Manager. I nomi di questi tag hanno il formato <PDM_...> o <pdm_...>.

Nota: per personalizzare i moduli CA Service Desk Manager con Screen Painter Web, non è necessario conoscere le estensioni HTMPL o lo stesso linguaggio HTML.

Ulteriori informazioni:

[Variabili del server](#) (a pagina 343)

[Tag HTMPL](#) (a pagina 321)

Convenzioni per la denominazione dei modelli

Le convenzioni per la denominazione seguenti sono usate per identificare i quattro tipi di base di file HTMPL, dove xxx è l'oggetto:

Tipo di modello	Nome
Elenco (filtro e risultati della ricerca)	list_xxx.htmpl

Tipo di modello	Nome
Modulo dettagli in sola lettura e in modifica combinate (interfaccia Analista)	detail_xxx.html
Modulo dettagli in sola lettura	detail_xxx_ro.html
Modulo dettagli in modifica	detail_xxx_edit.html

È possibile trovare le definizioni degli oggetti e le loro proprietà nelle seguenti posizioni:

- (UNIX) \$NX_ROOT/bopcfg/majic/*.maj
- (Windows) *directory-installazione*\bopcfg\majic*.maj

Per informazioni sugli oggetti e sugli attributi che definiscono CA Service Desk Manager, vedere la *Guida di riferimento tecnico di CA Service Desk Manager*.

Directory HTML

La *Guida all'amministrazione* descrive le interfacce Web fornite con CA Service Desk Manager. Vengono forniti diversi set di file HTML per implementare queste interfacce, come mostrato nella tabella seguente:

Sistema operativo	Directory contenente i file HTML
Windows	<i>Directory-installazione</i> \bopcfg\www\html\web\interfaccia
UNIX	\$NX_ROOT/bopcfg/www/html/web/interfaccia

In questa tabella, *interfaccia* è il nome dell'interfaccia (Analista, Cliente o Dipendente).

Nota: non esiste una directory separata per i file dell'interfaccia per gli utenti Guest; per impostazione predefinita, questa interfaccia usa i file dell'interfaccia Dipendente. È possibile cambiare l'interfaccia per gli utenti Guest modificando il tipo di accesso associato all'utente System_Anonymous. Sia i file dell'interfaccia Cliente che quelli dell'interfaccia Dipendente si modificano dinamicamente a seconda se l'utente corrente è un utente conosciuto o un utente Guest, tramite il comando <PDM_IF> descritto in questo documento.

Nella directory html, vi sono altre tre sottodirectory delle interfacce:

default:

Contiene i file HTML comuni a tutte le interfacce. Quando si cerca un file, il motore Web cerca prima nella directory corrispondente all'interfaccia dell'utente corrente, quindi nella directory default.

pda/analyst: (UNIX)**pda\analyst: (Windows)**

Contiene i file HTML usati dall'interfaccia per dispositivi mobili. In Unicenter Service Desk r11.0, l'interfaccia per dispositivi mobili è fornita solo per gli analisti.

web/interfaccia/legacy: (UNIX)**web\interfaccia\legacy: (Windows)**

Contiene i file HTML della release precedente di CA Service Desk Manager che non sono più usati. Questa directory viene creata automaticamente se si esegue la migrazione di una release precedente al momento dell'installazione di CA Service Desk Manager. È possibile eliminare la directory legacy se i file personalizzati non fanno riferimento a nessuno dei file in essa presenti.

Si raccomanda di non modificare direttamente i file HTML forniti, ma di usare Screen Painter Web o di copiare manualmente il file che si desidera modificare nella directory site mods locale e modificare questa copia. Il server Web CA Service Desk Manager cerca un nuovo modulo nella directory site mods appropriata prima di controllare la directory di distribuzione. Le directory site mods standard per ogni interfaccia sono:

Sistema operativo	Directory per i file HTML modificati in locale
Windows	<i>directory- installazione\site\mods\www\html\interfaccia\interface</i>
UNIX	<i>\$NX_ROOT/site/mods/www/html/interfaccia/interfaccia</i>

Nota: se si cambia un modulo e lo si salva nella directory *directory-installazione\site\mods\www\html\interface*, il modulo verrà visto da tutti, indipendentemente dal gruppo di moduli a cui appartiene. Se lo si salva nella directory *directory-installazione\site\mods\www\html\interface\interfaccia*, solo i contatti definiti come membri di quel gruppo di moduli lo potranno vedere.

Nella tabella precedente, *interfaccia* è il nome dell'interfaccia (Analista, Cliente o Dipendente). Non esiste una directory separata per i file dell'interfaccia per gli utenti Guest; questa interfaccia usa i file dell'interfaccia Dipendente. Il vantaggio di memorizzare nella directory site mods i file HTML modificati consiste nel fatto che questa directory viene conservata quando si installa un aggiornamento o un nuova release di CA Service Desk Manager. Inoltre, tenendo i file modificati nella directory site mods e conservando allo stesso tempo gli originali si è sicuri di disporre sempre di una copia corretta del file HTML distribuito in origine.

Ogni pagina dell'interfaccia Web ha una funzione principale, come indicato nella tabella seguente che elenca i modelli HTML principali. Tuttavia, è possibile aggiungere blocchi <PDM_FORM> a qualsiasi modello per accedere direttamente a qualsiasi operazione supportata dall'interfaccia Web. Ad esempio, è possibile modificare il menu principale per includere campi per l'invio di una questione senza usare la pagina intermedia o aggiungere campi di criteri di ricerca e un pulsante di ricerca a un modulo elenco:

Pagina Web	Modello HTML
Modulo principale	menu_frames.html
Visualizzazione/creazione/aggiornamento di un ordine di cambiamento	detail_chg.html
Visualizzazione di un elenco di ordini di cambiamento	list_chg.html
Visualizzazione/creazione/aggiornamento di una questione	detail_iss.html
Visualizzazione di un elenco di questioni	list_iss.html
Visualizzazione/creazione/aggiornamento di una richiesta	detail_cr.html
Visualizzazione di un elenco di richieste	list_cr.html
Visualizzazione di informazioni dettagliate sugli annunci	detail_cnote.html
Visualizzazione di un elenco di annunci	list_cnote.html
Eseguire l'accesso	login.html

Nota: per un elenco completo dei modelli, visualizzare il contenuto delle directory nella tabella all'inizio di questa sezione.

Gruppi modulo Web

È possibile raccogliere pagine Web personalizzate in uno o più gruppi di moduli. Le directory dei gruppi di moduli sono contenute nelle directory seguenti:

Windows

directory-installazione\site\mods\www\html\web\interfaccia

directory-installazione\site\mods\www\wwwroot\subdirectory

UNIX

\$NX_ROOT/site/mods/www/html/web/interfaccia

\$NX_ROOT/site/mods/www/wwwroot/subdirectory

Ogni gruppo di moduli è una sottodirectory di queste directory. La directory del modulo personalizzato viene specificata nel campo Personalizzazione gruppo moduli del tipo di accesso.

Quando un utente richiede un modulo, il motore Web cerca prima nella directory del gruppo di moduli appropriata, quindi nella directory standard dell'interfaccia Web dell'utente e infine nella directory default. È possibile definire più di un tipo di accesso per la stessa interfaccia Web, ognuno con un gruppo di moduli personalizzati diverso. Ciò consente di definire alcuni moduli specializzati per tipi diversi di utente e di usare ancora la maggior parte dei moduli dell'interfaccia standard.

Un processo simile si verifica quando una pagina Web richiede un file da una delle sottodirectory di wwwroot (css, html, img o scripts). Il motore Web esamina un riferimento HTML del modulo CAisd/img/xxx.gif e lo converte in:

- /CAisd/sitemods/img/formgroup/xxx.gif
- /CAisd/sitemods/img/xxx.gif
- /CAisd/img/xxx.gif

selezionando il primo in cui trova xxx.gif.

Modalità di creazione di un gruppo di moduli Web

Completare i passaggi seguenti per creare un gruppo di moduli Web:

1. Se si desidera un gruppo di moduli oltre quelli predefiniti dell'interfaccia Analista, Cliente o Dipendente, creare un nuovo gruppo scegliendo Salva con nome dal menu File in Screen Painter Web e facendo clic sul pulsante Aggiungi gruppo moduli, nella finestra di dialogo Salva modulo con nome. Ad esempio, se si desidera fornire due versioni personalizzate separate dell'interfaccia Analista, è possibile creare gruppi di moduli chiamati Analyst1 e Analyst2 per gestirli. È possibile anche definire un nuovo gruppo di moduli se l'interfaccia che si sta definendo non si concilia logicamente con nessuno dei gruppi di moduli predefiniti.
2. Nell'interfaccia Web (non una sessione di anteprima di Screen Painter Web), selezionare Protezione, Tipi di accesso dal menu Amministrazione. Quindi fare clic su un tipo di accesso, o crearne uno nuovo, e usare l'elenco a discesa Personalizzazione gruppo moduli, nella finestra Dettagli tipo accesso, per assegnare un gruppo di moduli ad un tipo di accesso. CA Service Desk Manager determina il tipo di accesso quando un contatto accede e usa Personalizzazione gruppo moduli per stabilire dove cercare i moduli personalizzati nella struttura di directory site mods. Se il motore Web non trova un modulo nella directory dei gruppi di moduli, cerca prima nella directory standard per il tipo di accesso dell'utente e poi nella directory default.

3. In Screen Painter Web scegliere Salva dal menu File o copiare manualmente i file HTML personalizzati nella directory seguente:

In Windows: *directory-*

installazione\site\mods\www\html\web\nome_gruppo_moduli

In UNIX: *\$NX_ROOT/site/mods/www/html/web/nome_gruppo_moduli*

Dopo aver configurato un nuovo gruppo di moduli Web e copiato tutti i file di supporto nelle sottodirectory appropriate, è necessario riavviare il servizio Web affinché i cambiamenti abbiano effetto.

Tag HTML

PDM_EVAL: inserimento del valore di una variabile di preelaborazione

Il tag `pdm_eval` è usato per inserire il valore di una variabile di preelaborazione nell'input del parser del motore Web. Se usata all'interno di una macro, l'effetto viene ritardato fino al completamento della macro.

Il tag `pdm_eval` funziona in modo simile a `pdm_include` o `pdm_macro`. Inserisce il testo nel parser in corrispondenza del tag, esattamente come se il valore della variabile fosse stato codificato al posto del tag.

La sintassi di `pdm_eval` è la seguente:

```
<PDM_EVAL TEXT=PRE.name>
```

nome

Obbligatorio; il nome della variabile di preelaborazione il cui valore deve essere inserito nell'input del motore Web.

PDM_FORM: avvio di un modulo HTML con un ID sessione

I tag `<PDM_FORM>` e `</PDM_FORM>` possono essere aggiunti a qualsiasi modello HTML dell'interfaccia Web per creare un modulo HTML che includa due campi nascosti per il SID (ID sessione) e il FID (ID modulo) delle variabili del server. L'operando OP crea un altro campo nascosto per una delle operazioni supportate, come con il tag `PDM_LINK`. Tranne nel caso dei campi nascosti generati automaticamente, `<PDM_FORM>` e `</PDM_FORM>` vengono usati allo stesso modo dei tag HTML standard `<form>` e `</form>` e generano questi tag come parte della loro espansione.

PDM_FMT: formattazione del testo inserito da una variabile del server

I tag <PDM_FMT> e </PDM_FMT> sono usati per formattare blocchi di testo inseriti dalle variabili del server (\$args.xxx) nel modo indicato dai relativi argomenti.

Nota: <PDM_FMT> è ignorato per i valori letterali, comprese le variabili \$prop.xxx.

La seguente tabella descrive questi tag:

Proprietà	Descrizione
ESC_STYLE= NONE	Specifica il tipo di escape del testo formattato. I valori validi sono:
C	NESSUNO
HTML	Impostazione predefinita. Specifica che non verrà applicato alcun trattamento speciale a nessun carattere nel corpo del contenuto.
JS	C
JS2	Applica un trattamento speciale ai caratteri ' , " , \ , \r , ` , e \n, che hanno un significato nei programmi in C. Questi caratteri verranno ignorati.
URL	HTML Applica un trattamento speciale ai caratteri seguenti, che hanno significato nel testo HTML: & diventa & ' diventa ' " diventa " < diventa < > diventa %gt; JS Applica un trattamento speciale ai caratteri seguenti, che hanno significato nel testo JavaScript: ' diventa %27 " diventa %22 / diventa %2F \ diventa %5C \r diventa %0D \n diventa %0A JS2

Proprietà	Descrizione
	Come JS, ma non applica alcun trattamento speciale al carattere / mentre applica un trattamento speciale ad altri due caratteri: - % diventa %25 - Le interruzioni di riga hanno %0A come suffisso URL Converte tutti i caratteri diversi da lettere, cifre e '@*-_.#' in '%xx', dove xx è la codifica esadecimale del carattere convertito.

Proprietà	Descrizione
JUSTIFY=LEFT CENTER RIGHT TRUNCATE WRAP LIN	Specifica la giustificazione del testo formattato. I valori validi includono: TRUNCATE Impostazione predefinita. Elimina la formattazione HTML sostituendo '<' e '>' con &lt; e &gt; Nota: per ulteriori informazioni, consultare le seguenti informazioni riguardo a KEEPLINKS e KEEPTAGS. LEFT CENTER RIGHT Produce esattamente i caratteri indicati da WIDTH, applicando troncamento o riempimento con spazi se necessario, sostituisce eventuali righe nuove incorporate con un solo spazio e delimita il testo di output con i tag [set the pre variable for your book] e </pre>. L'argomento WIDTH deve essere specificato come numero intero positivo. WRAP Come LEFT, tranne per il fatto che il testo viene portato a capo mantenendo intere le parole (le interruzioni di riga non vengono inserite all'interno delle parole). LINE Come TRUNCATE, tranne per il fatto che sostituisce anche tutte le interruzioni di riga incorporate con tag
.
KEEPLINKS=YES NO	Se si specifica KEEPLINKS=YES, l'azione di JUSTIFY=LINE o JUSTIFY=TRUNCATE viene modificata per conservare i tag di ancoraggio HTML (Azione:) mentre vengono convertiti tutti gli altri caratteri '<' e '>'. KEEPLINKS e KEEPTAGS si escludono a vicenda.
KEEPNL=YES NO	L'azione normale di PDM_FMT consiste nel convertire in uno spazio singolo tutte le nuove righe incorporate e qualsiasi spazio successivo. Se viene specificato KEEPNL=YES, le nuove righe incorporate verranno conservate. Questo argomento è ignorato da JUSTIFY=LINE.
KEEPTAGS=YES NO	Se si specifica KEEPTAGS=YES, l'azione di JUSTIFY=LINE o di JUSTIFY=TRUNCATE viene modificata per conservare tutti i tag HTML. KEEPTAGS e KEEPLINKS si escludono a vicenda.
PAD= YES NO	Se si specifica PAD=NO, PDM_FMT non converte le stringhe vuote in un singolo spazio. Questa è l'azione normale quando il valore di WIDTH è diverso da zero o JUSTIFY è TRUNCATE o WRAP.

Proprietà	Descrizione
WIDTH= <i>nn</i>	Quando il valore è diverso da zero, specifica che il testo deve essere formattato esattamente con i caratteri indicati da WIDTH.

<PDM_FMT> senza WIDTH o JUSTIFY non formatta il testo racchiuso ma lo delimita con [set the pre variable for your book] e </pre>.

Ad esempio, per generare una descrizione a più-righe, specificare:

```
<PDM_FMT WIDTH=50 JUSTIFY=WRAP>$args.description</PDM_FMT>
```

Per generare un output a più-colonne, specificare:

```
<PDM_FMT><PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.last_name</PDM_FMT>
<PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.first_name</PDM_FMT>
<PDM_FMT WIDTH=20 JUSTIFY=TRUNCATE>$cst.middle_name</PDM_FMT>
</PDM_FMT>
```

PDM_IF: elaborazione condizionale

Questi tag sono usati per includere testo sotto determinate condizioni. I blocchi <PDM_IF> possono essere inseriti ovunque in un file HTML, nel codice HTML, nel codice JavaScript e perfino all'interno dei tag HTML. Sia <PDM_IF> che <PDM_ELIF> (else if) stabiliscono una semplice clausola condizionale con le rispettive proprietà invece che con coppie nome-valore. Se la clausola è True, il testo racchiuso dai tag viene inserito nel file; se la clausola è False, il server ignora il testo racchiuso tra i tag. Il tag di chiusura può essere <PDM_ELIF>, <PDM_ELSE> o </PDM_IF>.

I tag <PDM_ELSE> e <PDM_ELIF> sono opzionali. Se vengono specificati entrambi, tutti i tag <PDM_ELIF> devono precedere <PDM_ELSE>. È possibile inserire un numero qualsiasi di tag <PDM_ELIF> tra <PDM_IF> e <PDM_ELSE> (o </PDM_IF> se è omesso <PDM_ELSE>).

La sintassi dell'espressione condizionale in <PDM_IF> e <PDM_ELIF> è la seguente:

- 0 è False; qualsiasi altro numero è True
- "" è False; *"qualsiasi -stringa"* è True
- *"valore op valore"* confronta tra loro i valori a sinistra e a destra secondo *op*. Se entrambi i valori sono costituiti da numeri (opzionalmente preceduti da - o +), i confronti vengono eseguiti numericamente. In caso contrario, il confronto è di tipo lessicale (confronto ASCII). I valori *op* validi includono:

Valore op	Descrizione
==	Uguale a
!=	Diverso da
>=	Uguale a o maggiore di (deve essere scritto \>= o >=)
<	Minore di (deve essere scritto \< o <=)
>	Maggiore di (deve essere scritto \> o >=)
<=	Uguale a o minore di (deve essere scritto \<= o <=)
&	Esegue un'operazione di tipo bit-and dei valori di destra e di sinistra. Il valore è True se sono impostati dei bit; False se non sono impostati bit.
%	Restituisce il valore True se il valore di sinistra è un multiplo pari del valore di destra e False nel caso contrario (utile per la creazione di tabelle bi-dimensionali).
:	Consente di eseguire una corrispondenza motivo orientata ai byte simile al comando grep di UNIX. Restituisce il valore True se il valore di sinistra contiene l'espressione regolare definita dal valore di destra.

Esempio:

```
<PDM_IF $count\>= 10> ...
<PDM_ELIF $count &lt; 5> ...
<PDM_ELSE> ...
</PDM_IF>
```

In un'istruzione PDM_IF può esserci più di un'espressione condizionale. Le espressioni condizionali sono separate dai connettori && (and) o || (or). Per l'utilizzo dei connettori non è necessario rispettare alcuna precedenza. Il motore Web esamina un'espressione condizionale da sinistra a destra finché non raggiunge il connettore. Se la condizione iniziale è True e il connettore è ||, il motore considera come True l'intera condizione senza eseguire altre valutazioni. Se la condizione iniziale è False e il connettore è &&, il motore considera come False l'intera condizione, senza eseguire altre valutazioni. In caso contrario, considera la condizione non determinata e valuta l'espressione condizionale dalla posizione del connettore in avanti.

PDM_INCLUDE: inserimento di testo da un file diverso

Il tag <PDM_INCLUDE> è usato per inserire testo da un secondo file in un file HTML. Il server sostituisce il tag <PDM_INCLUDE> con il contenuto del secondo file.

I file inclusi possono a loro volta contenere tag <PDM_INCLUDE>. Non c'è limite al livello di nidificazione.

Il tag <PDM_INCLUDE> supporta le proprietà seguenti:

Proprietà	Descrizione
FILE=filename	Obbligatoria; specifica il file da includere. Il motore Web esegue la ricerca nelle directory usate per i file HTML, come definito nel tipo di accesso dell'utente corrente.
FIXUP=[YES NO]	Opzionale; indica se il file deve essere interpretato dall'interfaccia Web come un normale file modello HTML, ad esempio che espande le variabili che iniziano con il simbolo del dollaro (\$) e interpreta altri tag CA Service Desk Manager come PDM_LIST e PDM_FORMAT. Il valore YES indica che il file deve essere considerato come un normale file modello HTML mentre il valore NO significa che il file incluso deve essere considerato come testo normale. Il valore predefinito è YES. Nota: per assicurare la compatibilità con le release precedenti, è possibile sostituire YES con TRUE o 1 e NO con FALSE o 0. Comunque non è opportuno usare questi valori nelle pagine nuove.
propname=value	Indica che la proprietà propname deve avere il valore specificato. È possibile accedere al valore della proprietà all'interno del file incluso aggiungendo a propname il prefisso \$prop. Ad esempio, la specifica

Proprietà	Descrizione
	seguente consente al file incluso di fare riferimento a \$prop.menubar: <PDM_INCLUDE ... menubar=no> Le proprietà globali possono anche essere specificate nel file di configurazione web.cfg. Per ulteriori informazioni su web.cfg, vedere la <i>Guida all'amministrazione</i> . Nota: per assicurare la compatibilità con le release precedenti, i valori della proprietà specificati in <PDM_INCLUDE> possono essere richiamati senza il prefisso 'prop.', nella forma \$propname. Comunque non è opportuno non usare il prefisso nelle pagine nuove.

PDM_JSCRIPT: inclusione condizionale di un file JavaScript

Il tag <PDM_JSCRIPT> è usato per includere in un modulo, sotto determinate condizioni, un file JavaScript. Questo tag ha due formati:

```
<PDM_JSCRIPT file=xxx.js [include=yes|no]>
```

La specifica pdm_jscript file=xxx.js indica che il file JavaScript xxx.js è richiesto da questo modulo. Il motore Web aggiunge il file a un elenco di file JavaScript richiesti dal modulo. L'elaborazione del tag avviene quando il modulo viene analizzato e non è interessata da pdm_if. Cioè, un tag pdm_jscript che fa riferimento a un file aggiunge quel file all'elenco dei file JavaScript se è presente in un punto qualsiasi del file, di un file incluso o di una macro.

È possibile specificare l'argomento opzionale *include=no* per indicare di ignorare il tag. Questo argomento fornisce l'elaborazione condizionale per il tag ed è utile soprattutto quando il tag viene richiamato in una macro. Ad esempio, la macro dtlTextbox specifica:

```
<PDM_JSCRIPT file=spellcheck.js include=&{spellchk}>
```

Ciò indica che qualsiasi modulo contenente una macro dtlTextbox che specifica spellchk=yes richiede il file JavaScript spellcheck.js.

Il secondo formato del tag pdm_jscript è:

```
<PDM_JSCRIPT insert=here>
```

Pdm_jscript con insert=here chiede al motore Web di inserire i tag HTML <script> standard per tutti i file JavaScript richiesti. Il motore Web elabora questo formato del tag durante la fase di generazione HTML, in modo che sia interessato da pdm_if. Un tag pdm_jscript insert=here è parte di std_head_include.html, pertanto è presente praticamente in ogni modulo.

Nota: il motore Web inserisce i tag script solo la prima volta che incontra pdm_jscript insert=here.

PDM_LINK: creazione di un collegamento ipertestuale che richiama un'operazione HTML

È possibile aggiungere i tag `<PDM_LINK>` e `</PDM_LINK>` a qualsiasi modello HTML di interfaccia Web per creare collegamenti che richiamano un'operazione HTML. Il tag `<PDM_LINK>` genera il tag HTML `<a href=...>` standard e ha argomenti simili tranne per il fatto che consente la specifica di un'operazione CA Service Desk Manager invece di un URL.

Il formato è il seguente, dove *operazione* è una delle operazioni supportate:

```
<PDM_LINK OP=operazione> ... </PDM_LINK>
```

Esempio:

```
<PDM_LINK OP=MENU> Menu </PDM_LINK>
```

```
<PDM_LINK OP=CREATE_NEW_FACTORY=iss> Invia questione </PDM_LINK>
```

```
<PDM_LINK OP=LOGOUT> Disconnetti </PDM_LINK>
```

PDM_LIST: formattazione di un elenco di righe del database

I tag `<PDM_LIST>` e `</PDM_LIST>` sono usati per delimitare le sezioni HTML che si ripetono per generare un output a più-record. Tutto quanto è compreso tra `<PDM_LIST>` e `</PDM_LIST>` viene ripetuto una volta per ogni record da generare. Esistono due tipi di `PDM_LIST`:

- Elenchi ricavati da un attributo di un oggetto che implica un elenco. Ad esempio, l'attributo `properties` dell'oggetto `request` è l'elenco delle proprietà associate a quella richiesta. Questo tipo di `PDM_LIST` ha sempre la proprietà `SOURCE`.
- Elenchi con una clausola `WHERE` esplicita. Questo tipo di `PDM_LIST` ha sempre la proprietà `WHERE`.

Un `<PDM_LIST>` di un attributo di un oggetto ha le proprietà seguenti:

Proprietà	Descrizione
<code>ESC_STYLE=NONE</code>	Specifica il tipo di escape del testo formattato. I valori validi sono:
<code>C</code>	NESSUNO
<code>HTML</code>	Impostazione predefinita. Specifica che non verrà applicato alcun trattamento speciale a nessun carattere nel corpo del contenuto.
<code>JS</code>	C
<code>JS2</code>	Applica un trattamento speciale ai caratteri <code>'</code> , <code>"</code> , <code>\</code> , <code>\r</code> , <code>'</code> e <code>\n</code> , che hanno un significato nei programmi in C. Questi caratteri verranno ignorati.
<code>URL</code>	HTML
	Applica un trattamento speciale ai caratteri seguenti, che hanno significato nel testo HTML:
	<code>&</code> diventa <code>&amp;</code>

Proprietà	Descrizione
	' diventa &apos; " diventa &quot; < diventa &lt; > diventa &gt; JS Applica un trattamento speciale ai caratteri seguenti, che hanno significato nel testo JavaScript: ' diventa %27 " diventa %22 / diventa %2F \ diventa %5C \r diventa %0D \n diventa %0A JS2 Come JS, ma non applica alcun trattamento speciale al carattere / mentre applica un trattamento speciale ad altri due caratteri: - % diventa %25 - Le interruzioni di riga hanno %0A come suffisso URL Converte tutti i caratteri diversi da lettere, cifre e '@*-_.#' in '%xx', dove xx è la codifica esadecimale del carattere convertito.
LENGTH= <i>nn</i>	Specifica il numero di righe dell'output (il valore predefinito è tutto).
PREFIX= <i>prefisso</i>	Specifica il prefisso nei riferimenti agli attributi nei record dell'elenco. Il riferimento ha il formato <i>\$prefisso.nome_attr</i> nel testo compreso tra <PDM_LIST> e </PDM_LIST>. La proprietà PREFIX è opzionale in un elenco di variabili degli oggetti. Se si omette PREFIX, viene usato anche il valore di SOURCE per il prefisso.
SEARCH_TYPE=DISPLAY GET_DOB	Specifica il metodo che il server deve usare per generare il modulo elenco: DISPLAY specifica che il server deve emettere una singola query per tutto il modulo GET_DOB specifica che il server deve emettere query separate per ogni riga del modulo La scelta influenza le prestazioni dell'elenco e dipende dalla complessità dell'elenco (il numero di unioni richieste per visualizzarlo) e dalle caratteristiche del DBMS. Le prestazioni di GET_DOB sono più controllabili di quelle di DISPLAY e infatti costituisce il valore

Proprietà	Descrizione
	predefinito.
<code>SORT=nome-indice</code>	Specifica il nome dell'indice da usare per l'ordinamento. Il valore predefinito di questo argomento è DEFAULT (che indica il primo indice di ordinamento per il factory sottostante).
<code>SOURCE=fonte</code>	Specifica la variabile dell'oggetto che definisce questo elenco. Questo campo è obbligatorio. Non inserire il simbolo del dollaro (\$) davanti a <i>origine</i> nell'istruzione PDM_LIST. Se non è specificata la proprietà PREFIX, il valore <i>origine</i> è usato anche come prefisso per i riferimenti agli attributi nei record dell'elenco, nei riferimenti nel formato <i>\$origine.nome_attr</i> . Se usato in un riferimento, <i>origine</i> non richiede il simbolo del dollaro.
<code>START=nn</code>	Specifica la prima riga dell'output (zero è il valore predefinito).

Esempio:

```

<table border>
<tr>
<th>Numero ordine di cambiamento figlio</th>
<th>Riepilogo</th>
</tr>
<PDM_LIST SOURCE=args.children>
<tr>
[assign the value for TD in your book]$args.children.chg_ref_num</td>
[assign the value for TD in your book]$args.children.summary</td>
</tr>
</PDM_LIST>
</table>

```

Poiché non sono stati specificati prefissi, i riferimenti agli attributi dei record nell'elenco hanno il prefisso \$args.children, il valore origine.

Un PDM_LIST di una clausola WHERE ha le proprietà seguenti:

Proprietà	Descrizione
<code>FACTORY=nome</code>	Specifica una classe dell'oggetto da ricercare. Questa proprietà è obbligatoria.
<code>LENGTH=nn</code>	Specifica il numero di righe dell'output (il valore predefinito è tutto).
<code>ORDER_BY=nome-attr</code>	Specifica il nome dell'attributo in base al quale effettuare l'ordinamento. Può contenere i modificatori DESC (decrescente) o ASC (crescente).
<code>PREFIX=prefisso</code>	Specifica il prefisso nei riferimenti agli attributi nei record dell'elenco. I riferimenti hanno il formato <i>\$prefisso.nome_attr</i> nel testo compreso tra <PDM_LIST> e </PDM_LIST>. La proprietà PREFIX è obbligatoria

Proprietà	Descrizione
	in un elenco della clausola WHERE.
START= <i>nn</i>	Specifica la prima riga dell'output (zero è il valore predefinito).
WHERE= <i>clausola-WHERE</i>	Specifica la clausola WHERE per la ricerca. Può contenere attributi (notazione a punti). Questa proprietà è obbligatoria.

Ad esempio:

```
<table>
<tr>
<th>Numero ordine di cambiamento figlio</th>
<th>Riepilogo</th>
</tr>
<PDM_LIST PREFIX=list FACTORY=chg WHERE="status = 'OP'">
<tr>
[assign the value for TD in your book]$list.chg_ref_num</td>
[assign the value for TD in your book]$list.summary</td>
</tr>
</PDM_LIST>
</table>
```

PDM_MACRO: inserimento di testo da un file macro

Tag PDM_MACRO

Il tag <PDM_MACRO> è usato per inserire un file macro in un file HTML. Funzionalmente è simile a PDM_INCLUDE ma con due importanti differenze:

- Un file incluso da PDM_MACRO ha un elenco formale di argomenti, obbligatori e con valori predefiniti.
- Un file incluso da PDM_MACRO proviene sempre dalla directory specificata dalla proprietà di configurazione MacroPath, indipendentemente dal tipo di accesso dell'utente corrente.

NAME=*nomemacro*

Obbligatoria; specifica la macro da includere. Il motore Web inserisce il suffisso ".mac" e cerca il file nel percorso specificato dalla proprietà MacroPath del file di configurazione.

A seconda della macro inclusa, possono essere necessarie altre proprietà. Il layout generale di un file macro è:

```
commenti
#args
name1 [= value1]
name2 [= value2]
...
#data
data to insert
```

Le descrizioni seguenti spiegano il layout del file, riga per riga:

- **commenti**—Le uniche istruzioni valide in una macro prima dell'istruzione `#args` sono i commenti. I commenti sono indicati da un segno `#` o `//` come primo carattere diverso dallo spazio.
- **#args**—Deve essere scritta esattamente così, con il segno `#` a colonna uno e nessun'altra informazione sulla riga. Questa istruzione inizia la sezione "args" che può contenere definizioni degli argomenti e commenti.
- **nome [= valore]**—Definisce un argomento per la macro. Per la macro sono validi solo gli argomenti citati esplicitamente nella sezione "args". Un valore specificato per un argomento nella sezione "args" costituisce il valore predefinito di quell'argomento. Gli argomenti privi di valore predefinito sono obbligatori e devono essere forniti dal file chiamante nella stessa istruzione `<PDM_MACRO>`.
- **#data**—Deve essere scritta esattamente così, con il segno `#` a colonna uno e nessun'altra informazione sulla riga. Questa istruzione inizia la sezione "data", che è parte della macro inserita nel file usando `PDM_MACRO`. Tutto il contenuto della sezione "data" viene inserito nel file chiamante, comprese le righe dei commenti prima della sezione "data".
- **dati da inserire**—I dati da inserire nel file chiamante. Questi dati possono contenere riferimenti ad argomenti nel formato:
- **&{arg_name}**—Questi riferimenti sono sostituiti dal valore dell'argomento fornito dal file chiamante o dal valore predefinito, in assenza del valore del chiamante.

Il motore Web generalmente legge un file macro una sola volta, la prima in cui viene usato, e quindi conserva la macro analizzata nella propria memoria. Ciò migliora le prestazioni ma può essere scomodo nel caso la macro sia in fase di sviluppo. Usare la proprietà `SuppressMacroCache` del file di configurazione per impedire questo comportamento e far sì che il motore Web elimini tutte le macro in memoria ogni volta che inizia l'elaborazione di un nuovo modulo.

Per escludere i tag PDM_MACRO dall'elaborazione

Per escludere i tag <PDM_MACRO> dall'elaborazione, inserire un punto esclamativo davanti alla P, come segue: <!PDM_MACRO>. Per impedire che il browser elabori la parte del modulo esclusa, inserire <PDM_IF 0> prima del tag <!PDM_MACRO> e </PDM_IF> dopo la riga esclusa.

Esempio:

```
<PDM_IF 0>
```

```
<!PDM_MACRO NAME=dtlDropdown hdr="Status" attr=status lookup=no  
evt="onBlur=\\\"detailSyncEditForms(this)\\\"">  
<!PDM_MACRO NAME=dtlDropdown hdr="Priority" attr=priority lookup=no  
evt="onBlur=\\\"detailSyncEditForms(this)\\\"">
```

```
</PDM_IF>
```

Macro predefinite utilizzate da Screen Painter Web

CA Service Desk Manager include numerose macro predefinite. La maggior parte di esse inserisce testo JavaScript per creare un elemento su un modulo Web. Usare Screen Painter Web per creare e modificare i moduli che utilizzano queste macro.

Macro dei moduli dettagli

button

Inserisce un pulsante grafico.

dtlCheckbox

Inserisce una casella di controllo su un modulo dettagli.

dtlDate

Inserisce un campo per la data su un modulo dettagli.

dtlDateReadonly

Inserisce un campo per la data di sola lettura su un modulo dettagli.

dtlDropdown

Inserisce un elenco a discesa su un modulo dettagli.

dtlEnd

Termina un modulo dettagli.

dtlEndTable

Termina una tabella all'interno di un modulo dettagli.

dtlForm

Inizia un modulo dettagli.

dtlHTMLEditBox

Inserisce un campo del modulo dettagli che è una casella di testo contenente un editor HTML.

dtlHier

Inserisce un campo del modulo dettagli che è una casella di testo convalidata rispetto a una tabella esterna con una ricerca gerarchica.

dtlLookup

Inserisce un campo del modulo dettagli che è una casella di testo convalidata rispetto a una tabella esterna.

dtlLookupReadOnly

Inserisce un campo del modulo dettagli che è un collegamento ipertestuale di sola lettura a una tabella esterna.

dtlReadOnly

Inserisce un campo di testo di sola lettura su un modulo dettagli.

dtlStart

Inizia la prima tabella in un modulo dettagli.

dtlStartExpRow

Inizia una riga espandibile su un modulo dettagli.

dtlStartRow

Inizia una riga normale su un modulo dettagli.

dtlTextbox

Inserisce una casella di testo su un modulo dettagli.

contactLookup

La macro contactLookup consente di creare una ricerca contatti. Tale macro include gli argomenti seguenti:

```
contactLookup("&{header}","&{frameName}","&{factory}","&{lookupName}");
```

header

Identifica l'intestazione della ricerca.

frameName

(Obbligatorio) Identifica il nome del modulo

factory

Specifica il factory.

Impostazione predefinita: agt

lookupName

(Obbligatorio) Identifica il nome della ricerca.

È anche possibile abilitare e disabilitare questo elemento specificando:

```
contactLookupDisable( Name, bDisable )
```

bDisable=

- true
Disabilita l'elemento.
- false
Abilita l'elemento.

dtlCheckboxReadonly

La macro dtlCheckboxReadonly specifica un campo casella di controllo di sola lettura in un modulo dettagli HTML. La macro include gli argomenti seguenti:

```
detailCheckboxReadonly("&{hdr}","&{attr}",&{colspan},"$args.&{attr}", "&{on}", "&{off}");
```

hdr

Specifica il testo dell'intestazione.

Impostazione predefinita: "\$args.&{attr}.DISPLAY_NAME"

attr

(Obbligatorio) Specifica il nome dell'attributo.

on = "X"

Specifica il valore visualizzato nel modulo di sola lettura quando si seleziona il campo.

off = ""

Specifica il valore visualizzato nel modulo di sola lettura quando non si seleziona il campo.

colspan = 1

Specifica il numero di colonne del modulo.

Nei moduli di sola lettura e di modifica il campo viene visualizzato come specificato negli argomenti "on" e "off".

Nota: questa macro è simile a dtlCheckbox.mac, con l'eccezione che è sempre di sola lettura, anche in modalità di modifica.

Macro dei moduli elenco

IsCol

Specifica una colonna in un modulo elenco.

IsEnd

Termina la parte dell'elenco in un modulo elenco.

IsStart

Inizia la parte dell'elenco in un modulo elenco.

IsWrite

Inserisce testo nella sezione che si ripete di un modulo elenco.

sfDate

Inserisce un campo per la data in un filtro di ricerca.

sfDropdown

Inserisce un elenco a discesa in un filtro di ricerca.

sfEnd

Termina un filtro di ricerca.

sfHier

Inserisce un campo del filtro di ricerca che è una casella di testo convalidata rispetto a una tabella esterna con una ricerca gerarchica.

sfLookup

Inserisce un campo del filtro di ricerca che è una casella di testo convalidata rispetto a una tabella esterna.

sfStart

Inizia un filtro di ricerca.

sfStartRow

Inizia una riga all'interno di un filtro di ricerca.

sfTextbox

Inserisce una casella di testo in un filtro di ricerca.

Macro per barra dei menu

endMenu

Termina un menu all'interno di una barra dei menu.

menuItem

Definisce una voce globale in un menu.

endMenubar

Termina una barra dei menu.

menuItemLocal

Definisce la voce di un menu richiamata nel contesto della finestra corrente.

menubarItem

Definisce un menu all'interno di una barra dei menu.

startMenu

Inizia un menu all'interno di una barra dei menu.

startMenubar

Inizia una barra dei menu.

PDM_NOTEBOOK: creazione di un notebook

Diversi moduli nell'interfaccia Analista di CA Service Desk Manager usano un controllo notebook. Un notebook consente la presenza in una stessa area dello schermo di più insiemi di campi ma la visualizzazione di un solo insieme alla volta. L'utente seleziona il set di campi visibile facendo clic su una determinata scheda nella parte superiore del notebook o premendo la combinazione di tasti `Alt+n`, dove *n* è il numero della scheda. Dettagli questione (`detail_iss.html`) è un esempio di modulo che usa un notebook. È consigliato l'utilizzo di Screen Painter Web per modificare i contenuti dei notebook o inserire un notebook in un modulo che non ne contenga già uno.

Il tag `</PDM_NOTEBOOK>` contrassegna la fine di un notebook. Si consiglia di specificare questo tag al fine di garantire la compatibilità con le release future. Comunque in questa release l'uso è opzionale e non genera codice di output.

PDM_PRAGMA: specificazione delle informazioni sul server

Il tag `<PDM_PRAGMA>` è usato per specificare informazioni usate dal motore Web, ad esempio il rilascio e la release di un modulo. Non genera codice HTML e può essere inserito ovunque in un modulo. Gli argomenti utilizzabili sono:

Argomento	Descrizione
RELEASE=value	Specifica il numero di release CA Service Desk Manager corrispondente a questo modulo. Questo valore è "110" in tutti i moduli Unicenter Service Desk r11.0. È accessibile all'interno del modulo, nella variabile <code>\$prop.release</code> .
SITEMOD=value	Specifica una stringa definita a livello di sito che identifica le modifiche applicate a questo modulo. È accessibile all'interno del modulo, nella variabile <code>\$prop.sitemod</code> .
VERSION=value	Specifica una stringa definita da CA che identifica il numero di versione di questo modulo. È accessibile all'interno del modulo, nella variabile <code>\$prop.version</code> .
OVERIDE=YES NO	Specifica se i valori in questa istruzione PDM_PRAGMA devono sostituire i valori nelle precedenti istruzioni PDM_PRAGMA.

CA usa le istruzioni PDM_PRAGMA per documentare le versioni dei moduli. Tutti i moduli di Unicenter Service Desk r11.0 includono l'istruzione PDM_PRAGMA seguente:

```
<PDM_PRAGMA RELEASE=110>
```

Inoltre, il modulo `std_head.html` include l'istruzione JavaScript seguente:

```
cfgFormRelease = "$prop.release" - 0;
```

L'istruzione PDM_PRAGMA e la variabile cfgFormRelease consentono all'interfaccia Web di CA Service Desk Manager di distinguere i moduli r11.0 da quelli di release precedenti. Le release precedenti a r6.0 non supportavano l'istruzione PDM_PRAGMA.

Normalmente, per impostare set \$prop.release, \$prop.sitemod e \$prop.version vengono usate solo le istruzioni PDM_PRAGMA nel file di livello massimo di un modulo (cioè un file non richiamato da PDM_INCLUDE). Inoltre, un'istruzione PDM_PRAGMA non sostituisce un valore non vuoto impostato da una precedente istruzione PDM_PRAGMA. È possibile impostare OVERRIDE=YES per specificare che un'istruzione PDM_PRAGMA può sostituire precedenti istruzioni PDM_PRAGMA o che è possibile usare un'istruzione PDM_PRAGMA in un file incluso.

PDM_SCOREBOARD: creazione di una struttura segnapunti

Il tag <PDM_SCOREBOARD> è usato per generare il segnapunti mostrato sul lato sinistro del modulo principale. Ha la proprietà seguente:

TARGET=valore

Specifica il nome del frame di destinazione per gli elenchi richiesti facendo clic su un nodo presente nel contatore. Gli elenchi vengono caricati nella destinazione specificata, che può essere qualsiasi valore supportato per l'attributo di destinazione di un collegamento. Il valore predefinito è *_self* (la finestra contenente il tag PDM_SCOREBOARD).

Qualsiasi modulo HTML che include un tag <PDM_SCOREBOARD> deve includere anche il file fldtree.js JavaScript. Questo file può essere incluso tramite l'istruzione seguente nella sezione <HEAD> del modulo:

```
<SCRIPT LANGUAGE="JavaScript" SRC="$CAisd/CAisd/fldtree.js"></SCRIPT>
```

Inoltre, è opportuno includere un collegamento chiamato scoreboard_asof_data per visualizzare la data di validità dei numeri nella struttura. Per un esempio dell'uso di questo tag, vedere il file scoreboard.html distribuito.

Le query incluse nel segnapunti sono definite dal contenuto della tabella User_Query (con nome oggetto usq) per l'utente corrente. Un record in questa tabella definisce ogni riga nella struttura (cartella o nodo).

Inizialmente, gli utenti non hanno voci associate nella tabella User_Query. Un utente senza voci User_Query riceve il set predefinito di query segnapunti associato al proprio tipo di accesso. Un utente con autorizzazione di amministratore può anche personalizzare il segnapunti predefinito per un tipo di accesso.

PDM_SET: impostazione del valore di una variabile del server

Il tag <PDM_SET> è usato per assegnare un valore a una variabile del server. La sintassi è la seguente:

<PDM_SET arg.nome[+]=value>

arg

Obbligatorio; specifica il tipo di variabile e deve essere arg per l'uso normale.

Nota: non vi sono caratteri \$.

Nome

Obbligatorio; specifica il nome della variabile.

+

Opzionale; specifica che il valore deve essere aggiunto alla fine del valore esistente della variabile. Non sono ammessi spazi né prima né dopo.

=

Obbligatorio; deve essere specificato esattamente come indicato, senza spazi né prima né dopo.

valore

Obbligatorio; specifica il testo da assegnare o aggiungere alla fine della variabile.

Il tag PDM_SET può essere usato anche nella fase di preelaborazione per creare o aggiornare una variabile di preelaborazione.

Ulteriori informazioni:

[Preelaborazione del motore Web](#) (a pagina 369)

PDM_TAB: creazione di una scheda in un notebook

Il tag <PDM_TAB> viene usato per definire una scheda del notebook. È consigliato l'utilizzo di Screen Painter Web per modificare i contenuti dei notebook o inserire un notebook in un modulo che non ne contenga già uno.

PDM_WSP: controllo dell'anteprima Web Screen Painter

Il tag <PDM_WSP> viene usato per controllare la funzione di anteprima di Screen Painter Web. Non genera codice HTML e può essere inserito ovunque in un modulo.

Per impostazione predefinita, Screen Painter Web determina come visualizzare l'anteprima di un modulo dal nome del modulo:

- Per i moduli dettagli (*detail_factory.html*), Screen Painter Web visualizza il modulo nella vista di modifica, con i dati ricavati dalla riga creata per ultima della tabella appropriata. Se non vi sono dati che si possono visualizzare nella tabella, Screen Painter Web visualizza il modulo predisposto per creare una nuova riga. Notare che le sessioni di anteprima di Screen Painter Web normalmente non possono aggiornare il database. Screen Painter Web visualizza i moduli nella vista di modifica per consentire di vedere in anteprima tutte le funzioni. Tuttavia, CA Service Desk Manager ignora le richieste di salvataggio da una sessione di anteprima di sola lettura. Per questo il motore Web cambia il testo del pulsante Salva in noSave.
- Per i moduli elenco (*list_factory.html*), Screen Painter Web visualizza il modulo nella vista di elenco, con i dati ricavati dalla riga creata per ultima della tabella appropriata. Se non vi sono dati che si possono visualizzare nella tabella, Screen Painter Web visualizza il modulo nella vista di ricerca, con il filtro aperto.
- Per gli altri moduli, Screen Painter Web visualizza semplicemente il modulo, senza contesto del database.

È possibile modificare questo comportamento predefinito inserendo un tag PDM_WSP in un punto qualsiasi del modulo. Ad esempio, è possibile visualizzare una scheda del notebook nel relativo modulo dettagli o fornire argomenti obbligatori per i moduli normalmente richiamati con un ambiente fornito da un altro modulo. Sono possibili i seguenti argomenti:

Proprietà	Descrizione
FACTORY= <i>valore</i>	Specifica il factory del motore oggetti usato da questo modulo.
PREVIEW= <i>nome.html</i> <i>valore</i> no	Specifica l'URL di anteprima. Può essere il nome di un file HTML, nel formato <i>xxxx.html</i> , un URL CA Service Desk Manager (usato senza modifiche se inizia con "OP=") o la parola chiave "no" che indica che il modulo non può essere visualizzato in anteprima. Un valore che non inizia con OP= viene modificato sostituendo un riferimento del modulo { <i>factory</i> } o { <i>factory:</i> } rispettivamente con un ID o con un ID persistente della riga creata per ultima del factory a cui si fa riferimento e che può essere visto dall'utente corrente.
WHERE= <i>valore</i>	Specifica una clausola WHERE usata per cercare una o più righe

Proprietà	Descrizione
	rappresentative da mostrare nel modulo in anteprima.
MODE= <i>valore</i>	Specifica la posizione dell'URL costruita. Può avere questa forma: ■ GENERAL. Formato generale: Determina la modalità esaminando l'argomento anteprima: detail_xxxx.html - READONLY list_xxxx.html - LIST qualsiasi altro - GRONK ■ READONLY. File dettaglio visualizzato in sola lettura. ■ EDIT. File dettaglio visualizzato in modifica. ■ LIST. File elenco. ■ GRONK. File non specificato. In questa situazione, disabilitare il file.

Variabili del server

Le informazioni su CA Service Desk Manager vengono incluse nel modello HTML usando variabili che iniziano con il simbolo del dollaro (\$). Ogni pagina viene creata con alcune variabili che sono documentate nel file modello. Queste variabili possono essere inserite nella pagina o usate in istruzioni condizionali:

- Variabili semplici
- Variabili delle proprietà
- Variabili di ambiente
- Variabili degli oggetti azienda
- Variabili degli elenchi

Variabili semplici

Le variabili semplici specificano i flag che vengono passati alla pagina Web. Per accedere a una variabile semplice, usare il nome preceduto dal simbolo del dollaro (\$). In questo modo si rende disponibile il valore della variabile. \$CAisd e \$cgi sono due esempi di questo tipo di variabile. Inserendo \$CAisd in un modello si sostituisce la directory di installazione del server Web CA Service Desk Manager principale, mentre \$cgi fa riferimento all'URL del programma pdmweb.exe. Le variabili semplici sono documentate nella sezione superiore del file HTML in cui sono usate.

Di seguito è riportato l'elenco delle variabili che possono essere usate in tutti i file HTML:

\$ACCESS.gruppo

L'oggetto privilegio di accesso dell'utente contiene le impostazioni dei privilegi nel *gruppo* funzionale per l'utente corrente. Ad esempio, \$ACCESS.admin gestisce il valore del privilegio per il gruppo funzionale admin. I valori dei privilegi validi sono:

- 0 (Nessun accesso)
- 1 (Visualizzazione)
- 2 (Modifica)

Questa variabile non è disponibile nel modulo di accesso.

\$cgi

L'URL del programma pdmweb.exe.

\$cst

L'oggetti dati dell'utente corrente. Questa variabile non è disponibile nel modulo di accesso. È possibile fare riferimento a singoli attributi di questo oggetto usando il formato *\$cst.nomeattr*; ad esempio, *\$cst.first_name*.

\$CAisd

L'URL della directory di installazione del server Web CA Service Desk Manager principale.

\$MachineName

Il MachineName definito nel file web.cfg.

Nota: per informazioni su web.cfg, vedere la *Guida all'amministrazione*.

\$ProductName

Il nome del prodotto definito nel file NX.env.

\$SESSION

L'oggetto sessione salva tutte le variabili di sessione includendo l'ID di sessione (\$SESSION.SID) e tutte le variabili definite dal file web.cfg.

Nota: per informazioni su web.cfg, vedere la *Guida all'amministrazione*.

\$USER_STATE

Informazioni sullo stato definito dall'utente.

Variabili delle proprietà

Le variabili delle proprietà rappresentano una proprietà del file di configurazione, web.cfg. È possibile accedere a qualsiasi voce nel file web.cfg (comprese voci definite dall'utente) all'interno di un file modello HTML aggiungendo il prefisso "\$prop."

Di seguito è riportato un esempio di una delle righe di web.cfg, che specifica il numero di voci visualizzate in una singola pagina in un modulo elenco:

```
ListPageLength 10
```

È possibile fare riferimento a questa variabile in un modello HTML specificando:

```
$prop.ListPageLength
```

Se si usa il tag speciale <PDM_INCLUDE> per incorporare un altro file in un file modello, è possibile specificare ulteriori proprietà come attributi del tag <PDM_INCLUDE>. È possibile fare riferimento a queste proprietà nel file incluso allo stesso modo usato per le proprietà di web.cfg. Una proprietà specificata come un attributo <PDM_INCLUDE> avente lo stesso nome di una proprietà di web.cfg sostituisce la proprietà di web.cfg nel file incluso.

Ad esempio, il tag seguente <PDM_INCLUDE> include una proprietà chiamata \$prop.menubar a cui si può fare riferimento all'interno del file std_body.html:

```
<PDM_INCLUDE FILE=std_body.html menubar=no>
```

Nota: è possibile fare riferimento a una proprietà del file di configurazione xxx in due modi: \$prop.xxx o \$SESSION.xxx. Entrambi restituiscono lo stesso valore. Tuttavia si preferisce la sintassi \$prop.xxx perché comporta un minore carico sul server.

Oltre alle proprietà di web.cfg, esistono diverse proprietà predefinite a cui si può accedere con \$prop. Esse sono:

\$prop.browser

Stringa che identifica il browser usato. Ad esempio "IE" per Internet Explorer.

\$prop.combo_name

Stringa contenente il nome dell'utente corrente, nel formato "last_name, first_name middle_name".

\$prop.factory

Stringa contenente il factory associato al modulo corrente, ad esempio "cr" per le richieste o "iss" per le questioni.

\$prop.FID

Stringa contenente l'ID numerico del modulo corrente.

\$prop.form_name

Stringa contenente il nome del modello HTML corrente, nel formato xxx.html.

\$prop.form_name_1

Stringa contenente la sottostringa del nome del modulo prima del primo trattino di sottolineatura. Ad esempio, per il modulo detail_chg_edit.html, form_name_1 è "detail".

\$prop.form_name_2

Stringa contenente la sottostringa del nome del modulo dopo il primo trattino di sottolineatura e prima dell'ultimo trattino di sottolineatura (o del punto). Ad esempio, per il modulo detail_chg_edit.html, form_name_2 è "chg".

\$prop.form_name_3

Stringa contenente la sottostringa del nome del modulo dopo l'ultimo trattino di sottolineatura e prima del punto. Per esempio, per il modulo detail_chg_edit.html, form_name_3 sarebbe "modifica". Per il modulo dettaglio combinazione , che ha un nome file del modulo detail_xxx.html, \$prop.form_name_3 è impostata sulla visualizzazione attuale, "sl" o "modifica".

\$prop.release

Stringa contenente il livello di release del modulo. L'istruzione PDM_PRAGMA contiene più dettagli su questa proprietà.

\$prop.SID

Stringa contenente l'ID numerico della sessione corrente.

\$prop.sitemod

Stringa contenente il nome della modifica definita in locale del modulo. L'istruzione PDM_PRAGMA contiene più dettagli su questa proprietà.

\$prop.user_type

Stringa contenente "analyst," "customer," "employee" o "guest".

\$prop.version

Stringa contenente la versione del modulo. L'istruzione PDM_PRAGMA contiene più dettagli su questa proprietà.

Ulteriori informazioni:

[PDM_PRAGMA: specificazione delle informazioni sul server](#) (a pagina 339)

Variabili di ambiente

Le variabili di ambiente rappresentano una voce nel file di configurazione NX.env. È possibile fare riferimento a qualsiasi voce del file NX.env all'interno di un file modello HTML inserendo il prefisso "\$env".

Di seguito è riportato l'esempio di una delle righe di NX.env, che specifica il nome host del server CA Service Desk Manager:

```
@NX_SERVER=hostname
```

È possibile fare riferimento a questa variabile in un file modello HTML specificando:

```
$env.NX_SERVER
```

Variabili degli oggetti azienda

Le variabili degli oggetti azienda rappresentano un oggetto CA Service Desk Manager, ad esempio una questione o una richiesta. Per accedere a un oggetto, è necessario iniziare con il nome della variabile, seguito da un punto (.) e da qualsiasi nome di attributo che si desidera visualizzare. Ad esempio, in una questione in cui, per convenzione, l'oggetto è rappresentato dalla variabile args, è possibile visualizzare la descrizione, la data di apertura, il numero di telefono dell'assegnatario, il numero di attività sulla questione e la descrizione della prima attività, come mostrato di seguito:

```
$args.description  
$args.open_date  
$args.assignee.phone_number  
$args.act_log.length  
$args.act_log.0.description
```

È possibile usare le parentesi graffe per delimitare il nome della variabile se non è circondato da spazi. Ad esempio, \$foo bar e \${foo}bar sono nomi validi. È possibile anche usare la variabile args per accedere a valori che non sono attributi (ad esempio, \$args.KEEP.*nome*, come descritto in Operazioni supportate).

Una variabile non attributo può non essere definita. Ad esempio, è possibile accedere a un modulo da due punti diversi, di cui solo uno fornisce un valore per \$args.KEEP.foo. È possibile specificare un valore predefinito per un riferimento \$args usando la sintassi seguente, in cui il riferimento è sostituito dalla stringa dopo i due punti se la *variabile* non è definita:

```
${args.variabile:default}
```

Variabili delle date con fuso orario

Le variabili delle date con fuso orario sono un tipo speciale di variabili degli oggetti azienda. Forniscono un mezzo per convertire le date in formato universale (UTC), rappresentate come numeri interi, in date in formato di stringa adattate al fuso orario del browser dell'utente. La variabile per rappresentare le date con numeri interi è:

`$args.nome_attr_INT_DATE`

Esempio: `$args.open_date_INT_DATE`

Variabili dei dati factory

Le variabili dei dati factory sono un tipo speciale di variabili degli oggetti azienda. Una variabile dei dati factory è sostituita dalle informazioni su un oggetto a cui si fa riferimento. Sono disponibili sette variabili di questo tipo:

`$args.nome_attr.COMMON_NAME`

Il nome comune (stringa leggibile dall'esterno) della tabella a cui fa riferimento l'attributo. Ad esempio, nel modulo Dettagli richiesta, il valore di `$args.assignee.COMMON_NAME` è il nome combinazione dell'assegnatario ("last, first, middle").

`$args.nome_attr.COMMON_NAME_ATTR`

Il nome dell'attributo del nome comune nella tabella a cui fa riferimento l'attributo. Ad esempio, nel modulo Dettagli richiesta, il valore di `$args.assignee.COMMON_NAME_ATTR` è il "combo_name".

`$args.FACTORY_nome_attr`

Il nome del factory associato all'attributo specificato. Ad esempio, nel modulo Dettagli richiesta, il valore di `$args.FACTORY_assignee` è "agt".

`$args.LENGTH_nome_attr`

La lunghezza massima dell'attributo. Ad esempio, nel modulo Dettagli richiesta, il valore di `$args.LENGTH_summary` è 240.

`$args.nome_attr.REL_ATTR`

REL_ATTR (chiave esterna) dell'attributo. Ad esempio, nel modulo Dettagli richiesta, il valore di `$args.assignee.REL_ATTR` è il valore del campo dell'ID dell'assegnatario.

`$args.nome_attr.REL_ATTR_ATTR`

Il nome dell'attributo di REL_ATTR nella tabella a cui fa riferimento l'attributo. Ad esempio, nel modulo Dettagli richiesta, il valore di `$args.assignee.REL_ATTR_ATTR` è "id".

\$args.REQUIRED_nome_attr

Una stringa, "0" o "1", indicante se è necessario l'attributo a cui si fa riferimento.

\$args.nome_attr.SELECTIONS

Un elenco di selezioni valide per *nome_attr*. Questo valore è una stringa vuota se *nome_attr* non è un riferimento a un'altra tabella o se la dimensione della tabella a cui fa riferimento *nome_attr* supera il valore della proprietà SelListCacheMax nel file di configurazione. Altrimenti la variabile SELECTIONS è una stringa contenente il nome comune e il REL_ATTR di tutte le voci nella tabella a cui si fa riferimento. I valori successivi sono separati dalla stringa "@,@", in modo che il valore della variabile abbia il formato:

"cname1@,@rel_attr1@,@cname2@,@rel_attr2"

\$args.factory_SEL_UNDER_LIMIT

Una stringa, "0" o "1", che indica se il numero corrente di righe nella tabella corrispondente a *factory* è minore del valore della proprietà SelListCacheMax nel file di configurazione. A questa variabile si preferisce la variabile SELECTIONS, che dovrebbe essere usata in tutti i nuovi moduli.

Il riferimento con notazione a punti presente nelle variabili dei dati factory (COMMON_NAME, REL_ATTR e SELECTIONS) può avere una lunghezza qualsiasi. Ad esempio, in un modulo Dettagli richiesta \$args.assignee.organization.COMMON_NAME viene sostituito dal nome esterno dell'organizzazione dell'assegnatario.

Variabili degli elenchi

Le variabili degli elenchi sono usate per eseguire iterazioni tra i dati. Vi si accede utilizzando tag elenco come descritto in PDM_LIST: formattazione di un elenco di righe del database.

Operazioni del server

Operazioni supportate

Per consentire l'integrazione delle pagine Web di CA Service Desk Manager con le proprie pagine Web, sono supportate le operazioni seguenti:

CREATE_NEW

Fornisce un'interfaccia generica per consentire all'utente di creare una nuova riga in una determinata tabella. È necessario specificare il nome dell'oggetto e, per impostazione predefinita, viene usato un modello chiamato *dettagli_xxx_edit.html* per l'oggetto *xxx*. È possibile ignorare il file *.html* specificando la proprietà HTML.

Specificatori obbligatori:

FACTORY=*object-name*

Specificatori opzionali:

ALG_PRESET=*espressione_preset*

ALG_PRESET_REL=*espressione_preset*

CREATE_ALG=*tipo_registro_attività*

HTML=*zdetailxxx_factory.html*

KEEP.*nome_attr*=*valore*

PRESET=*espressione_preset*

PRESET_REL=*espressione_preset*

SET.*nome_attr*=*valore*

use_template=1 | 0 (0 è il valore predefinito)

Nota: per usare lo specificatore HTML con CREATE_NEW, il modulo a cui si fa riferimento deve avere un nome conforme alla convenzione *zdetailxxx_factory.html*. Deve iniziare con la stringa *zdetail*, seguita da caratteri alfanumerici (compresa una stringa nulla), seguiti da un carattere di sottolineatura e dal nome del *factory*.

ENDSESSION o LOGOUT

Chiude la sessione di accesso corrente. ENDSESSION è l'operazione consigliata.

GENERIC_LIST

Fornisce un'interfaccia generica per consentire all'utente di visualizzare un elenco da qualsiasi tabella nel database. È necessario specificare il nome dell'oggetto e, per impostazione predefinita, viene usato un modello chiamato *list_xxx.html* per l'oggetto *xxx*. È possibile ignorare il file *.html* specificando la proprietà HTML.

Specificatori obbligatori:

FACTORY=*object-name*

KEEP.*nome_attr*=*valore*

DISPLAY_FORM

Fornisce un'interfaccia generica per consentire all'utente di visualizzare qualsiasi modulo personalizzato.

Specificatori obbligatori:

HTML=*file_html*

Nota: DISPLAY_FORM sostituisce JUST_GRONK_IT. Le implementazioni esistenti possono continuare a utilizzare JUST_GRONK_IT, che funziona esattamente come DISPLAY_FORM. DISPLAY_FORM è l'operazione consigliata.

MENU

Mostra la pagina di menù principale, definita nel file web.cfg nelle proprietà dei menù.

Specificatori opzionali:

HTML=*filemenu*

filemenu è il nomefile del menu principale alternativo.

PAGE_EXTENSION

Consente al Web master di specificare ulteriori estensioni per l'interfaccia.

Specificatori obbligatori:

NAME=*file_html*

html_file è uno dei nomi di file elencati nel file di configurazione UserPageExtensions.

Specificatori opzionali:

REQUIRES_LOGIN=1

Se presente, compare una pagina di accesso se l'utente non ha ancora effettuato l'accesso. Se manca o è impostato su zero, il file viene mostrato senza verificare se l'utente ha effettuato l'accesso.

RELOG

Visualizza la schermata di accesso.

SEARCH

Fornisce un'interfaccia generica per consentire l'esecuzione di ricerche in qualsiasi tabella del database. Questa operazione presuppone che sia stato creato un `search_XXX.html` appropriato, dove `XXX` è il *nome-oggetto*, come definito nei file `.maj` nella cartella `majic` in `bopcfg`.

Nota: per ulteriori informazioni, consultare la *Guida di riferimento tecnico di CA Service Desk Manager*. Per impostazione predefinita, i risultati di questa ricerca sono visualizzati in `list_XXX.html`, ma questo file può essere ignorato specificando la proprietà `HTML`.

Specificatori obbligatori:

```
FACTORY=nome-oggetto  
QBE.op.nome_attr=valore
```

Specificatori opzionali:

```
ALG_PRESET=espressione_preset  
ALG_PRESET_REL=espressione_preset  
CREATE_ALG=tipo_registro_attività  
HTML=file_elenco_html  
KEEP.nome_attr=valore
```

SEC_REFRESH

Aggiorna le informazioni sull'accesso dell'utente dal sottosistema di protezione. Agli utenti in possesso del privilegio di modifica (per il gruppo funzionale `admin`) viene fornito un collegamento ipertestuale per questa operazione sulla schermata del menu. Dopo aver aggiornato il privilegio di accesso di un utente usando il programma di protezione, con questa operazione è possibile aggiornare le informazioni sull'accesso (vengono aggiornate le informazioni di protezione per tutti gli utenti).

Nota: l'aggiornamento della protezione è un processo asincrono. Una volta completato, viene visualizzato un messaggio nel file registro standard (`stdlog`).

SET_MENU

Il comportamento di questa operazione è uguale a quello di `MENU`, quando `MENU` è usata con la variabile `HTML`. L'unica differenza è che questa operazione imposta anche il modulo menu predefinito sul modulo specificato con la proprietà `HTML`.

Specificatori obbligatori:

```
HTML=file_html
```

Nota: con questa operazione viene ignorata l'impostazione `MENU` nel file `web.cfg` finché il servizio Web non viene riavviato.

SHOW_DETAIL

Fornisce un'interfaccia generica per consentire all'utente di visualizzare in sola-lettura i dettagli di una riga in una determinata tabella. È necessario specificare il nome dell>ID persistente (da cui si ricava il nome dell'oggetto). Per impostazione predefinita, viene usato un modello chiamato `detail_xxx_ro.html` per l'oggetto `xxx`. È possibile ignorare il file `.html` specificando la proprietà HTML.

Specificatori obbligatori:

`PERSID=id-persistente`

Specificatori opzionali:

`ALG_PRESET=espressione_preset`

`ALG_PRESET_REL=espressione_preset`

`CREATE_ALG=tipo_registro_attività`

`HTML=file_dettagli_html_sola_lettura`

UPDATE

Fornisce un'interfaccia generica per modificare qualsiasi tabella. È necessario passare l>ID e il nome dell'oggetto; un modulo dettagli modificabile viene visualizzato dall'utente. Per impostazione predefinita, l'utente ha accesso esclusivo al record per due minuti e, se in questo periodo vengono inviati i cambiamenti, il database viene aggiornato.

Specificatori obbligatori:

`PERSID=id-persistente` o

`SET.id=id-riga-da-aggiornare` `FACTORY=nome-oggetto`

Specificatori opzionali:

`NEXT_PERSID=id-persistente` (del record da visualizzare dopo l'aggiornamento)

`KEEP.nome_attr=valore`

`KEY.nome_attr=valore`

`HTML=zdetailxxx_factory.html`

Nota: per usare lo specificatore HTML con UPDATE, il modulo a cui si fa riferimento deve avere un nome conforme alla convenzione `zdetailxxx_factory.html`. Il nome deve iniziare con la stringa "zdetail", seguita da caratteri alfanumerici (compresa una stringa nulla), seguiti da un carattere di sottolineatura e dal nome del factory.

Nota: per informazioni su `web.cfg`, vedere la *Guida all'amministrazione*.

Variabili delle operazioni

Questa tabella elenca le variabili che possono essere impostate per ogni operazione nelle operazioni supportate:

Variabili	Descrizione	Operazioni
ALG_PRESET ALG_PRESET_REL	Specifica i valori per uno o più attributi del registro attività creato come risultato della variabile CREATE_ALG. Se non si specifica CREATE_ALG, ALG_PRESET e ALG_PRESET_REL vengono ignorate.	CREATE_NEW SEARCH SHOW_DETAIL
CREATE_ALG	Specifica il tipo di registro attività da creare come effetto secondario dell'operazione. Usare le variabili ALG_PRESET o ALG_PRESET_REL per specificare i valori per gli attributi del nuovo registro attività. Il momento in cui viene creato il registro attività dipende dall'operazione: CREATE_NEW Il registro attività viene creato quando viene salvato il nuovo record. Se il nuovo record non viene salvato, non viene creato nessun registro. SEARCH Il registro attività viene creato quando viene selezionato un record dal modulo elenco. Se il record viene visualizzato ma non selezionato (cioè l'utente seleziona esplicitamente il comando Visualizza dal menu di scelta rapida del modulo elenco), non viene creato nessun registro. SHOW_DETAIL Il registro attività viene creato prima della visualizzazione del record.	CREATE_NEW SEARCH SHOW_DETAIL
FACTORY	Specifica la classe dell'oggetto da cercare, creare o aggiornare. È possibile usare qualsiasi nome specificato come OBJECT nei file *.maj in \$NX_ROOT/bopcfg, come riportato in Guida di riferimento tecnico di CA Service Desk Manager.	CREATE_NEW GENERIC_LIST SEARCH UPDATE
HTMPL	Consente all'autore dell'HTMPL di ignorare la convenzione per la denominazione dei modelli predefiniti e specificare esplicitamente il file HTMPL da visualizzare al posto del modello predefinito. Nota: quando viene usato lo specificatore HTMPL con CREATE_NEW o UPDATE, il nome del modulo a cui si fa riferimento deve essere conforme alla convenzione zdetailxxx_factory.html, dove xxx rappresenta	CREATE_NEW DISPLAY_FORM JUST_GRONK_IT MENU SEARCH SET_MENU SHOW_DETAIL UPDATE

Variabili	Descrizione	Operazioni
	qualsiasi carattere e <i>factory</i> è il nome del factory.	
KEEP. <i>nome</i>	Specifica il valore che può essere salvato e passato tra le pagine.	CREATE_NEW GENERIC_LIST SEARCH UPDATE
KEY. <i>nome_attr</i>	Simile a SET. <i>nome_attr</i> tranne per il fatto che specifica una ricerca in <i>nome_attr</i> , che deve essere un riferimento a un'altra tabella o oggetto.	UPDATE
NEXT_PERSID	Specifica l'ID persistente del successivo record da visualizzare.	UPDATE
PERSID	Specifica l'ID persistente del record da visualizzare. Questa variabile può essere specificata nei modi seguenti: Direttamente, con ID persistente composto dal nome di un factory, due punti (:) e un ID database, univoco e con numeri interi. Ad esempio, PERSID=chg:1234 specifica l'ordine di cambiamento con ID database 1234. Indirettamente, con un ID persistente composto dal nome di un factory, due punti (:), il nome di un attributo, due punti (:) e un valore. Questo formato di PERSID specifica il record del factory indicato che ha un attributo con il valore specificato. Ad esempio, PERSID=chg:chg_ref_num:demo:3 specifica l'ordine di cambiamento con numero di riferimento demo:3.	SHOW_DETAIL UPDATE
PRESET PRESET_REL	Specifica i valori per uno o più attributi del record creato come risultato della variabile CREATE_NEW. Se non si specifica CREATE_NEW, PRESET viene ignorato.	CREATE_NEW

Variabili	Descrizione	Operazioni
QBE.op.nome_attr	Specifica i valori da usare quando si esegue una ricerca. Questi valori vengono identificati per mezzo di una parola chiave QBE, dove <i>nome_attr</i> identifica qualsiasi nome di attributo che può essere impostato in un ticket e <i>op</i> indica di cercare le condizioni in cui l'attributo: EQ è uguale al valore NE è diverso dal valore GT è maggiore del valore LT è minore del valore GE è maggiore o uguale al valore LE è maggiore o uguale al valore NU è nullo NN non è nullo IN corrisponde all'espressione SQL LIKE KY contiene il testo immesso Se non si definisce nessuna variabile QBE, viene visualizzata la finestra standard di ricerca.	SEARCH
SET.nome_attr	Specifica il nome attributo da usare quando viene creato un ticket, dove <i>attr_name</i> identifica qualsiasi attributo in un ticket che può essere impostato. I nomi degli attributi variano in base all'oggetto sottostante. Tutti gli oggetti e i rispettivi attributi possono essere trovati nei file *.maj, nella directory majic in bopcfg, come riportato nella Guida di riferimento tecnico CA Service Desk Manager.	CREATE_NEW UPDATE
SET.id	Specifica l'ID della riga del database da aggiornare.	UPDATE
SKIPLIST	Se impostata su 1, non viene visualizzato l'elenco dei risultati delle ricerche che restituiscono un solo risultato. Vengono invece visualizzati direttamente i dettagli in sola lettura.	SEARCH
usa_modello	Se impostata su 1, l'operazione SEARCH restituisce un elenco di modelli. Il modello restituito selezionato verrà usato nell'operazione CREATE_NEW per inserire i dati in un nuovo record. Questa variabile è valida solo per gli ordini di cambiamento, le questioni e le richieste.	CREATE_NEW SEARCH

Ulteriori informazioni:

[Sintassi di PRESET, PRESET_REL, ALG_PRESET e ALG_PRESET_REL](#) (a pagina 357)

Sintassi di PRESET, PRESET_REL, ALG_PRESET e ALG_PRESET_REL

Le parole chiave PRESET, PRESET_REL, ALG_PRESET e ALG_PRESET_REL nell'URL specificano i valori iniziali per gli attributi del ticket e del relativo registro attività, rispettivamente. Sono disponibili due formati:

[ALG_]PRESET=attr:valore

Indica che l'attributo specificato del ticket o del registro attività deve essere impostato sul valore specificato. Ad esempio, la specifica seguente imposta la descrizione del nuovo ticket su "Hello:"

```
PRESET=description:Hello
```

[ALG_]PRESET_REL=attributo:oggetto.attributorel:attributotest:valore

Indica che l'attributo specificato del ticket o del registro attività deve essere impostato su un valore copiato da un'altra tabella del database. Il valore viene copiato dall'attributo *relattr* dell'*oggetto* il cui attributo *testattr* ha il *valore* specificato. Ad esempio, la specifica seguente imposta l'attributo analyst del nuovo ticket sull'ID del contatto il cui ID utente è xyz123:

```
PRESET_REL=analyst:cnt.id:user:xyz123
```

Quando viene usato questo formato, la query implicita deve recuperare un record univoco. Se nessuno o più di un contatto ha come ID utente xyz123, la specifica PRESET dell'esempio non ha effetto.

Per impostare più attributi in un URL è possibile usare più volte le parole chiave PRESET, PRESET_REL, ALG_PRESET e ALG_PRESET_REL. In alternativa, un singolo operando di parola chiave può specificare più valori separati da @@. Se viene usato il separatore '@@', non è possibile usare insieme i formati dei valori per le parole chiave [ALG_]PRESET e [ALG_]PRESET_REL. L'esempio seguente mostra due modi diversi di specificare i valori per description, summary e analyst del ticket:

```
PRESET=description:Hello+PRESET=summary:HelloThere+PRESET_REL=analyst:cnt.id:user:xyz123
PRESET=description:Hello@@summary:HelloThere+PRESET_REL=analyst:cnt.id:user:xyz123
```

Per richieste, questioni, incidenti, problemi e ordini di cambiamento, sia PRESET che PRESET_REL supportano l'attributo della parola chiave ASSET per collegare un oggetto a un asset. L'attributo ASSET aggiorna l'attributo *affected_resource* di una richiesta, incidente o problema oppure l'*LREL* dell'asset di una questione o ordine di cambiamento.

Esempi di collegamenti

Gli esempi di collegamenti seguenti non includono il percorso a CA Service Desk Manager. Tutti gli URL CA Service Desk Manager iniziano con questo formato di codice:

`http://hostname[:port]/CAisd/pdmweb.exe`

In questo esempio, *hostname* è il nome del server e *port* (opzionale) è il numero della porta se si usa Tomcat. Questa codifica è rappresentata da un'ellissi (...) negli esempi di URL seguenti:

- Per creare una richiesta con un utente finale interessato con userid tooda01, usare il seguente URL di esempio:
`...?OP=CREATE_NEW+FACTORY=cr+PRESET_REL=customer:cnt.id:userid:toda01`
- Per visualizzare un elenco di tutte le richieste assegnate a userid tooda01, usare il seguente URL di esempio:
`...?OP=SEARCH+FACTORY=cr+QBE.EQ.assignee.userid=toda01`
- Per mostrare il modulo dettagli per la richiesta 1234, usare i seguenti URL di esempio:
`...?OP=SHOW_DETAIL+FACTORY=cr+PERSID=cr:ref_num:1234` (vista di sola lettura)
`...?OP=UPDATE+FACTORY=cr+PERSID=cr:ref_num:1234` (vista di aggiornamento)

Nota: è possibile ignorare l'accesso senza verifica usando i servizi Web per l'autenticazione. Per informazioni sul metodo `getBopsid()` vedere la Guida di riferimento tecnico di CA Service Desk Manager.

Personalizzazione avanzata

Bisogna tenere presenti vari aspetti della personalizzazione di pagine Web se si sceglie di utilizzare strumenti diversi da Screen Painter Web per modificare HTML, o nel caso di requisiti di personalizzazione particolarmente insoliti. Tuttavia, si raccomanda vivamente di lavorare con Screen Painter Web per personalizzare le pagine Web di CA Service Desk Manager prima di provare un altro approccio. Screen Painter Web è in grado di eseguire la maggior parte delle operazioni di personalizzazione necessarie e gestisce automaticamente le operazioni ausiliarie, ad esempio inserisce gli aggiornamenti nella directory site mods e distribuisce i file pubblicati a tutti i server.

Motore Web e relativa cache

Per personalizzare le pagine Web, è utile conoscere la struttura del server Web CA Service Desk Manager. L'interfaccia Web usa un contenitore servlet J2EE, ad esempio Tomcat, o un server HTTP standard, ad esempio Apache o Microsoft Internet Information Server (IIS). Quando un utente richiede una pagina Web CA Service Desk Manager, il server HTTP richiama il programma pdmweb.exe.

Una volta avviato, pdmweb.exe stabilisce una connessione con un daemon CA Service Desk Manager (o il servizio Windows) chiamato motore Web. Il motore Web interpreta la richiesta dell'utente. Molte richieste esigono che il motore Web cerchi un file modello (HTMPL) e lo converta nell'HTML standard. Di solito, il processo di conversione richiede che il motore Web comunichi con un server CA Service Desk Manager per leggere o aggiornare il database e includere le informazioni sul database nell'HTML generato. Una volta completato l'HTML, il motore Web lo invia a pdmweb.exe, che lo invia a sua volta al browser dell'utente.

Per ottimizzare le prestazioni, il motore Web normalmente legge ogni file HTMPL una sola volta. Dopo aver analizzato il file e stabilito come convertirlo in HTML, il motore Web memorizza il file analizzato nella propria cache, riducendo notevolmente il tempo di elaborazione la volta successiva che il file viene richiesto. Sebbene la cache sia utile in un ambiente di produzione, nella fase di sviluppo può rivelarsi scomoda, in quanto i cambiamenti ai file HTMPL non hanno effetto finché il motore Web non viene riavviato o non viene usata l'utilità pdm_webcache. In un ambiente di sviluppo, è possibile specificare la proprietà del file di configurazione SuppressHtmlCache. Tuttavia, si consiglia di non sopprimere la cache HTMPL in un ambiente di produzione in quanto si ripercuote gravemente sul rendimento generale del motore Web.

Nota: per ulteriori informazioni, vedere la *Guida all'amministrazione*.

Le pagine Web servite da pdmweb.exe vengono generate leggendo i file HTMPL e usando questi file per generare l'HTML. I file modello HTML sono identificati dall'estensione .htmlpl. È possibile modificare tali file modello, e si conseguenza personalizzare le pagine Web di CA Service Desk Manager.

Utilità pdm_webcache

Usare l'utilità pdm_webcache per rimuovere uno o più moduli HTML dalla cache del motore Web. Il motore Web sarà costretto a caricare questi moduli dal disco al loro successivo utilizzo e i cambiamenti potranno avere effetto.

```
pdm_webcache [-f nome-modulo] [-g gruppo-moduli] [-i interfaccia] [-p processo] [-v]
```

-f nome-modulo

Specifica il nome del gruppo di moduli da rimuovere dalla cache, ad esempio detail_cr.html. Per selezionare più gruppi di moduli, è possibile usare '%' (o '*') come carattere jolly. Ad esempio, specificando:

```
-f detail%
```

vengono selezionati tutti i moduli dettagli.

Questo argomento è opzionale. Se omissso, vengono selezionati tutti i moduli nella cache.

-g gruppo-moduli

Specifica il nome del gruppo di moduli da rimuovere dalla cache, ad esempio Analista. Per selezionare più gruppi di moduli, è possibile usare '%' o '*' come carattere jolly. Ad esempio, specificando:

```
-g Anal%
```

vengono selezionati tutti i gruppi di moduli che iniziano con "Anal".

Questo argomento è opzionale. Se omissso, vengono selezionati tutti i gruppi di moduli nella cache.

-i interfaccia

Specifica il nome dell'interfaccia Web da rimuovere dalla cache, ad esempio Analista, Cliente o Dipendente. È possibile usare '%' o '*' come carattere jolly. Ad esempio, specificando:

```
-i a%
```

viene selezionata l'interfaccia Analista.

Questo argomento è opzionale. Se omissso, vengono selezionate tutte le interfacce nella cache.

-p processo

Specifica il nome del motore Web di cui si vuole modificare la cache, ad esempio web:local.

Questo argomento è opzionale. Se omissso, vengono selezionati tutti i motori Web.

-v

Specifica di dettagliare l'output. Se questo argomento viene specificato, pdm_webcache elenca il nome completo di ogni modulo rimosso dalla cache, nel formato:

interfaccia:gruppo-moduli:nome-modulo

Questo argomento è opzionale. Se omissso, pdm_webcache riporta solo il numero dei moduli rimossi dalla cache di ogni motore Web.

Modalità di modifica dei modelli HTML

Di solito è possibile apportare due tipi di cambiamento ai modelli HTML:

- È possibile apportare modifiche che saranno visibili all'utente ma che non saranno modificate dall'interfaccia Web prima della visualizzazione. Ad esempio, è possibile aggiungere un file GIF per il logo dell'azienda alle pagine dell'interfaccia Web (un "pass through") aggiungendo il riferimento al file modello appropriato oppure è possibile aggiungere codice JavaScript alla pagina per convalidare l'input. Tutti i cambiamenti apportati al file HTML che non sono contenute in un tag PDM, come definito di seguito, vengono passate inalterate nell'HTML restituito all'utente.
- È possibile modificare le sezioni sostituibili dei modelli. Ad esempio, è possibile aggiungere i dati di una nuova applicazione alla pagina dei dettagli della richiesta.

Vari tipi di voci di modelli permettono di realizzare quanto segue:

- Visualizzare le informazioni CA Service Desk Manager all'utente.
- Impostare una pagina di query.
- Creare collegamenti ad altre pagine CA Service Desk Manager usando i tag di collegamento.

File che non devono essere modificati

Determinati modelli HTML e file JavaScript contengono informazioni necessarie a molti moduli Web CA Service Desk Manager. Le informazioni in questi modelli dipendono dalla release e sono essenziali per il funzionamento dell'interfaccia Web CA Service Desk Manager. Pertanto questi file vengono sempre sostituiti quando viene rilasciata una nuova versione di CA Service Desk Manager; i cambiamenti apportati a questi file non rientrano nell'aggiornamento.

I modelli interessati da questa limitazione sono:

ahdtop.html

Contiene stili, script e variabili JavaScript usati nell'interfaccia Web CA Service Desk Manager. Questo file fa parte del frameset principale dell'interfaccia Web ed è sempre presente durante una sessione. Tutti i moduli CA Service Desk Manager hanno accesso alla variabile JavaScript ahdtop che fa riferimento alla finestra contenente ahdtop.html.

menu_frames.html

Definisce il frameset HTML usato dal modulo principale CA Service Desk Manager.

msg_cat.js

Contiene il testo di tutti i messaggi usati nei file JavaScript CA Service Desk Manager.

reports.html

Contiene i dati necessari ai report Web.

std_body.html

Contiene le informazioni standard usate all'inizio della sezione BODY della maggior parte dei modelli HTML.

std_footer.html

Contiene le informazioni standard usate alla fine della sezione BODY della maggior parte dei modelli HTML.

std_head.html

Contiene le informazioni standard usate all'inizio della sezione HEAD della maggior parte dei modelli HTML.

styles.html

Contiene gli stili CSS usati nell'interfaccia Web CA Service Desk Manager.

Sebbene non sia possibile modificare questi file direttamente, è possibile aggiungervi informazioni. Ogni file xxx.html con restrizioni (tranne menu_frames.html e reports.html) ha un file xxx_site.html corrispondente che è possibile personalizzare. Per esempio è possibile aggiungere informazioni aggiuntive al file ahdtop_site.html, o aggiungere nuovi messaggi personalizzando msg_cat_site.js.

Il file xxx_site.html corrispondente a ciascun file ad accesso limitato viene caricato dopo il file principale in modo da poter ignorare o modificare il JavaScript nel file principale. Prestare attenzione quando si aggiungono informazioni perché cambiamenti non appropriati a questi file possono causare problemi imprevisti all'interfaccia Web CA Service Desk Manager.

Ulteriori informazioni:

[Directory usate dal server HTTP](#) (a pagina 366)

Indicazioni per i nuovi file HTML

È possibile aggiungere propri file HTML all'interfaccia Web CA Service Desk Manager. Attenersi a queste indicazioni per essere certi che i file HTML funzionino correttamente con il resto dell'interfaccia CA Service Desk Manager:

1. Includere l'istruzione seguente in un punto qualsiasi della sezione <HEAD> del file. Questa istruzione deve seguire l'istruzione <TITLE> se presente. Definisce diverse variabili globali JavaScript richieste dall'interfaccia Web CA Service Desk Manager e inoltre registra la pagina nel gestore finestre CA Service Desk Manager:

```
<PDM_INCLUDE FILE=std_head.html>
```

2. Includere l'attributo seguente come parte del tag <BODY> del file. Questo attributo aiuta il gestore finestre CA Service Desk Manager a tenere traccia della pagina:

```
onUnload="deregister_window()"
```

3. Includere l'istruzione seguente all'inizio della sezione <BODY> del file. L'argomento "menubar=no" è opzionale; se specificato, elimina la barra dei menu CA Service Desk Manager:

```
<PDM_INCLUDE FILE=std_body.html [menubar=no]>
```

4. Includere l'istruzione seguente alla fine della sezione <BODY> del file.

```
<PDM_INCLUDE FILE=std_footer.html>
```

Modalità di aggiunta di informazioni sullo stato definite dall'utente

Molti clienti desiderano avere la possibilità di incorporare proprie informazioni sullo stato nelle pagine Web CA Service Desk Manager e che CA Service Desk Manager passi le informazioni sullo stato a tutte le pagine successive nel corso della sessione utente. Queste informazioni possono essere interrogate usando istruzioni condizionali nei file HTML.

Le informazioni sullo stato per una sessione utente vengono inserite impostato l'attributo speciale USER_STATE nei collegamenti o nei moduli. Una volta inviata al motore Web CA Service Desk Manager, ogni pagina presentata all'utente avrà a disposizione la variabile HTML USER_STATE che sarà impostata sull'ultimo valore inviato per USER_STATE.

Gli esempi seguenti mostrano come è possibile impostare una voce in CA Service Desk Manager da un altro punto del sito, ad esempio dalle pagine destinate al personale addetto alle vendite:

- Uso di un collegamento ipertestuale

```
<a href="/CAisd/pdmweb.exe?USER_STATE=Sales">Service Desk</a>
```

- Uso di un modulo con un campo nascosto

```
<form action="http://host.com/CAisd/pdmweb.exe">  
<input type=hidden name=USER_STATE value=Sales>
```

Fare clic sul pulsante per Service Desk

```
<input type=submit>  
</form>
```

Quindi è possibile personalizzare i moduli HTML in base alle informazioni sullo stato:

```
<PDM_IF "$USER_STATE" == "Sales">  
    informazioni personalizzate per il personale di vendita  
  
<PDM_ELIF "$USER_STATE" == "Engineering">  
    informazioni personalizzate per i tecnici  
  
<PDM_ELSE>  
    informazioni per chiunque altro  
  
</PDM_IF>
```

Modalità di creazione di una richiesta direttamente da un modello

È possibile creare una nuova richiesta direttamente da un modello usando un URL.

Esempio

```
http://nomemacchina/CAisd/pdmweb.exe?FACTORY=cr+OP=CREATE  
NEW+PERSID=cr:3106+use_template=1
```

dove cr:3106 è il persid del modello.

Modalità di configurazione di un ticket di chiusura rapida con informazioni predefinite

Nella vista del Profilo rapido è possibile creare un ticket Chiusura rapida, ad esempio un Incidente chiusura rapida. Aggiungere una stringa preimpostata all'URL quando si crea un ticket Chiusura rapida per aggiungere una descrizione, un riepilogo o altre informazioni di campo automaticamente.

Per aggiungere una stringa preimpostata alla funzionalità del ticket Chiusura rapida, completare i passaggi seguenti:

1. Copiare il file `ahdtop_site.html` da `NX_ROOT/bopcfg/www/html/default` a `NX_ROOT/site/mods/html/www/default`.
2. Modificare il file [ahdtop_site.html file](#) (a pagina 365) con la variabile appropriata, a seconda del tipo di ticket Chiusura rapida.
3. Accedere a CA Service Desk Manager.
4. Creare un ticket Chiusura rapida.

Le informazioni preimpostate vengono aggiunte al ticket.

Creazione di un ticket di chiusura rapida con opzioni preimpostate

In Profilo rapido è possibile creare un ticket Chiusura rapida, ad esempio un Incidente chiusura rapida. L'opzione Chiusura rapida consente di aprire e chiudere un nuovo ticket in un solo passaggio, ad esempio quando si apre e si risolve l'incidente nella stessa sessione. È possibile aggiungere una stringa preimpostata all'URL quando si crea un ticket Chiusura rapida per aggiungere una descrizione, un riepilogo o altre informazioni di campo automaticamente.

Per creare un ticket di chiusura rapida con opzioni preimpostate

1. Copiare il file `ahdtop_site.html` da `NX_ROOT/bopcfg/www/html/default` a `NX_ROOT/site/mods/html/www/default`.
2. Modificare il file `ahdtop_site.html` per aggiungere la variabile appropriata, a seconda del tipo di ticket Chiusura rapida, con la stringa preimpostata.

- Incidente chiusura rapida: `var quick_close_preset_in`
- Problema chiusura rapida: `var quick_close_preset_pr`
- Richiesta chiusura rapida: `quick_close_preset_cr`
- Problema chiusura rapida: `quick_close_preset_iss`

La stringa seguente, ad esempio, consente di impostare la descrizione su `HelloIncident` e il riepilogo su `HelloIncidentSummary` per un Incidente chiusura rapida.

```
var quick_close_preset_in = "PRESET=description:HelloIncident@@summary:HelloIncidentSummary";
```

3. Accedere a CA Service Desk Manager.
4. Nella scheda Service Desk, selezionare Visualizza, Profilo rapido.
Viene visualizzata la pagina Ricerca rapida contatto profili.
5. Compilare uno o più campi di ricerca per il contatto e fare clic su Cerca.
L'Elenco contatti profilo rapido viene compilato con i contatti che corrispondono ai criteri di ricerca.
6. Selezionare un contatto.
Il riquadro di destra mostra le informazioni per il contatto.
7. Fare clic su Chiusura rapida.
Il ticket viene creato con le informazioni preimpostate.

Directory usate dal server HTTP

L'installazione predefinita di CA Service Desk Manager definisce due directory virtuali per il server HTTP:

- La directory virtuale CAisd punta alla directory seguente nell'installazione CA Service Desk Manager:
In Windows: *directory- installazione*bopcfg\www\wwwroot
In UNIX: \$NX_ROOT/bopcfg/www/wwwroot
- La directory virtuale CAisd/sitemods punta alla directory seguente nell'installazione CA Service Desk Manager:
In Windows: *directory-installazione*site\mods\www\wwwroot
In UNIX: \$NX_ROOT/site/mods/www/wwwroot

Le sottodirectory di queste directory virtuali sono:

Sottodirectory	Contenuto
css	Fogli di stile
help	Guida dell'interfaccia Web
html	file HTML
img	File grafici
scripts	JavaScript
sitemods	Personalizzazioni definite a livello di sito

Se si decide di creare una versione personalizzata di un file qualsiasi nelle directory `css`, `html`, `img` o `scripts`, si raccomanda di non aggiornare il file in `/CAisd`. Al contrario, memorizzare il file nella sottodirectory appropriata di `/CAisd/sitemods`. Ad esempio, se si decide di modificare un foglio di stile in `/CAisd/css`, memorizzare la versione personalizzata in `/CAisd/sitemods/css`. Quando il motore Web analizza i file HTML, modifica automaticamente i nomi file che iniziano con `$CAisd` in modo che puntino a `sitemods` se il file esiste in una sottodirectory di `sitemods`.

L'uso della directory `/CAisd/sitemods` comporta tre vantaggi:

- Consente di tenere traccia dei file distribuiti che sono stati modificati.
- Facilita l'accesso alla versione originale nel caso si verifichi un problema.
- Facilita il processo di gestione dell'installazione di una nuova release dato che l'installazione CA Service Desk Manager non inserisce nessun file nella directory `/CAisd/sitemods`.

Nota: non esiste una sottodirectory `/CAisd/sitemods/help`. Poiché i dati della Guida si trovano in file HTML standard (non nei modelli HTML), il motore Web non può modificare dinamicamente i riferimenti ai file. Se è necessario personalizzare la Guida, è necessario apportare cambiamenti in `/CAisd/help`.

La sottodirectory HTML contiene pochi file molto usati che non devono essere elaborati dal motore Web e possono migliorare le prestazioni se inseriti nella cache del browser. Se si crea una versione personalizzata di questi file, verificare attentamente che non contengano riferimenti ad altri file personalizzati. Poiché non avviene alcuna elaborazione da parte del motore Web, è necessario inserire manualmente un riferimento a `sitemods` dove appropriato.

Scaricamento allegati PDF

Quando si scarica e si visualizza un allegato PDF in CA Service Desk Manager, il file PDF può non essere visualizzato correttamente, o può aprirsi una finestra vuota dopo aver aggiornato alla versione Adobe Acrobat 7.0 o 8.0. Con CA Service Desk Manager, è possibile mostrare il file PDF correttamente realizzando i seguenti passaggi:

1. Impostare il parametro *forceDecompressOnDownload* su SÌ in `$NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml`.

Nota: in Linux, `$NX_ROOT` è `/opt/CAisd`

2. Riavviare i servizi CA Service Desk Manager.

Ricerca di informazioni nelle tabelle di riferimento

I campi di input su un modulo di dettaglio che modifica un record del database sono chiamati SET.attr_name. Quando il record è salvato, i dati dai campi SET vengono copiati direttamente al record sottostante. Pertanto, un campo di input per un attributo che fa riferimento a un'altra tabella deve contenere il valore REL_ATTR (chiave esterna) di quella tabella. Di solito si tratta dell'id, del persistent_id o del codice del record di riferimento.

Gli utenti non forniscono direttamente i valori REL_ATTR e i campi SET per gli attributi che fanno riferimento a un'altra tabella sono nascosti. Il campo visibile sul modulo è chiamato KEY.nome_attr e contiene il nome comune del record a cui fa riferimento. Un nome comune deve essere convertito in un valore REL_ATTR per aggiornare il record. Ciò può essere effettuato in questi casi:

- Per i campi con un elenco a discesa, il valore SET è fornito direttamente dall'elenco a discesa.
- Per i campi con una ricerca, quando un utente fa clic sulla ricerca e seleziona una voce, il valore SET viene copiato dalla voce selezionata.
- Per i campi con una ricerca in cui l'utente fornisce una chiave parziale che identifica in modo univoco il record e quindi fa clic sull'etichetta, il browser richiede il valore SET al server e copia sia il valore che l'intera chiave nel modulo.
- Se si specifica la proprietà Riempimento automatico del file di configurazione o si usa quella predefinita e l'utente fornisce una chiave parziale che identifica in modo univoco il record e fa clic su Notebook per uscire dal campo, il browser richiede il valore SET al server e copia sia il valore che l'intera chiave nel modulo.

Altrimenti, quando il record viene salvato con un valore KEY e nessun valore SET, il motore Web risolve il valore durante il salvataggio. Se non è possibile risolvere nessun valore KEY in un valore univoco SET, il salvataggio non avviene e viene visualizzato di nuovo il modulo di modifica.

Se un modulo viene rivisualizzato a seguito di un mancato salvataggio dovuto all'impossibilità di risolvere una ricerca, le variabili seguenti sono disponibili nell'HTML per ogni campo attributo cercato:

LIST_attr

Contiene tutte le corrispondenze trovate. Di solito è specificata a destra del campo SOURCE= in un'istruzione <PDM_SELECT>.

FLAGS_attr

È impostata su uno dei valori seguenti:

0

Visualizza il campo di ricerca iniziale.

1

È stato trovato un numero di corrispondenze maggiore di una e minore del valore di MaxSelectList (di solito, in questo caso, viene visualizzato l'elenco <PDM_SELECT>).

2

Non è stata trovata nessuna corrispondenza.

3

Sono state trovate troppe corrispondenze (più di MaxSelectList).

SEARCH_STATUS_attr stringa

Contiene la stringa di testo TooManyMatches dal file web.cfg.

Nota: per informazioni su web.cfg, vedere la *Guida all'amministrazione*.

Specificazione di ricerche sui contatti

Quando si specifica un contatto (nome, cognome e secondo nome) in un modulo modificabile, è possibile delimitare il nome del contatto con virgole (,) o spazi ma non con entrambi. È preferibile usare le virgole in quanto spesso i nomi contengono degli spazi e ciò potrebbe causare problemi.

Poiché non è possibile usare virgole e spazi in combinazione, l'uso delle virgole deve essere applicato a tutte le parti del nome; in assenza di virgole, i nomi vengono delimitati da spazi.

Dato che le informazioni alla fine vengono passate a una query SQL, il simbolo di percentuale (%) funge da carattere jolly. Ad esempio, 'P%, J%' può restituire 'Public, John', 'Penxa, Jane' e altri nomi i cui cognomi iniziano per P e i nomi per J. (La distinzione tra maiuscole e minuscole dipende dal database sottostante). Analogamente, 'P% J%' restituiranno gli stessi nomi.

Tuttavia, 'P%, Jon D' non restituisce tutti i contatti con nome Jon, iniziale del secondo nome D e cognome che inizia per P in quanto la presenza di una virgola fa sì che questa sia considerata l'unico delimitatore. Pertanto verrebbero cercati i cognomi 'P%' e il nome 'Jon D'. Per evitare questo errore, specificare 'P%, Jon, D'.

Preelaborazione del motore Web

Il motore Web funziona in due fasi durante l'elaborazione di un file HTML:

- La fase di preelaborazione, in cui legge il file HTML e tutti i file a cui fa riferimento (inclusi i file richiamati dai tag PDM_INCLUDE e PDM_MACRO). L'output della preelaborazione è una voce nella cache interna al motore Web.
- La fase di generazione, in cui legge il modulo dalla cache e genera l'HTML. L'output della generazione è l'HTML passato al browser.

La fase di preelaborazione di solito avviene una sola volta per ogni modulo nel corso dell'attività del motore Web. La fase di generazione avviene ogni volta che viene richiesto un modulo.

Durante la fase di preelaborazione è possibile usare i tag PDM_SET e PDM_EVAL per generare e memorizzare le informazioni, come il testo HTML, utilizzabili dal motore Web nella fase di generazione.

Variabili di preelaborazione

Le variabili di preelaborazione iniziano con la stringa "\$PRE.". Vengono create e aggiornate con il tag PDM_SET. La sintassi di questo tag, usato con una variabile di preelaborazione, è la seguente:

```
<PDM_SET PRE.nome[+]=value>
```

Questo tag assegna o aggiorna una variabile di preelaborazione, creandola se necessario. Viene elaborato quando il motore Web lo incontra leggendo un modulo. Solo le istruzioni PDM_IF invarianti interessano il PDM_SET di una variabile di preelaborazione; le altre vengono ignorate.

Rilevamento di istruzioni PDM_IF invarianti

Quando analizza un modulo, il motore Web rileva le istruzioni PDM_IF invarianti. Un'istruzione PDM_IF invariante è un'istruzione il cui argomento è costituito interamente da variabili letterali, di ambiente, di preelaborazione e di proprietà costanti. Quando il motore Web rileva un'istruzione PDM_IF invariante, ne valuta immediatamente la condizione. Le conseguenze sono:

- I tag PDM_SET e PDM_EVAL non elaborati da un'istruzione PDM_IF invariante vengono ignorati. Notare che tutti gli altri tag `pdm_eval` e `PDM_SET` che fanno riferimento alle variabili di preelaborazione vengono eseguiti al momento dell'elaborazione, anche se si trovano all'interno di un'istruzione PDM_IF non invariante.

- I riferimenti alle variabili del modulo non elaborati da un'istruzione PDM_IF invariante vengono ignorati e il loro valore non viene caricato quando viene usato il modulo. È possibile utilizzare questa tecnica per migliorare le prestazioni di un modulo. Ad esempio, se un modulo contiene i seguenti dati, il motore Web carica il valore di \$args.def prima di visualizzarlo:

```
<PDM_IF "$env.NX_OTB_MARKET == "itil" && "$args.a" == 1>  
<h1>This is form $args.def</h1>  
</PDM_IF>
```

Tuttavia, se viene scritto il seguente segmento, il motore Web determina che il primo PDM_IF è invariante e recupera il valore di \$args.def solo se \$NX_OTB_MARKET è "itil".

```
<PDM_IF "$env.NX_OTB_MARKET == "itil">  
<PDM_IF "$args.a" == 1>  
<h1>This is form $args.def</h1>  
</PDM_IF>  
</PDM_IF>
```

PDM_EVAL: inserimento del testo di una variabile di preelaborazione

Il tag PDM_EVAL inserisce il valore di una variabile di preelaborazione nell'input per il parser del motore Web. Se usata all'interno di una macro, l'effetto viene ritardato fino al completamento della macro.

Il tag PDM_EVAL funziona in modo simile a PDM_INCLUDE o PDM_MACRO. Inserisce il testo nel parser in corrispondenza del tag, esattamente come se il valore della variabile fosse stato codificato al posto del tag.

La sintassi di PDM_EVAL è la seguente:

```
<PDM_EVAL text=PRE.nome>
```

dove PRE.nome specifica il nome della variabile di preelaborazione il cui valore deve essere inserito nell'input del motore Web.

L'esecuzione del tag PDM_EVAL può essere controllata dalle istruzioni PDM_IF invarianti.

Importante su UNIX, è necessario impostare LIBPATH prima di eseguire l'utilità. Usare pdm_task per realizzare questa operazione. Per esempio, prima di avviare l'utilità, eseguire "pdm_task pdm_eval".

Personalizzazione libera dei moduli dettagli

Uso di JavaScript sui moduli dettagli

È possibile usare Screen Painter Web per aggiungere campi propri a un modulo dettagli oppure per ridisporre o modificare le caratteristiche dei campi forniti sul modulo per impostazione predefinita. Talvolta può essere necessario personalizzare un modulo non limitandosi alla semplice aggiunta di campi a una griglia. Con CA Service Desk Manager sono disponibili numerose funzioni JavaScript che facilitano l'inserimento di proprie personalizzazioni in un modulo dettagli di combinazione e strutturarne l'aspetto come si preferisce. Queste funzioni sono riepilogate come segue:

- È possibile inserire codice HTML in qualunque punto prima dell'istruzione `DetailForm()` o dopo l'istruzione `endDetail()` senza influire sul funzionamento del modulo dettagli.
- Per chiudere la tabella che definisce gli elementi del modulo dettagli sotto forma di griglia, è possibile usare la funzione `detailEndTable()`. Una volta compiuta questa operazione, è possibile disporre il codice HTML nel formato desiderato. In tal caso, il codice HTML e i campi nel modulo vengono inviati al motore Web quando l'utente fa clic su Salva. È possibile definire la funzione `detailNextID()` per generare i campi ID per gli elementi HTML che consentono ai campi di partecipare alla navigazione senza mouse del modulo dettagli. Le schede Notebook contengono diversi esempi di questa tecnica, ad esempio `xx_alg_tab.html`.
- È possibile inserire una macro `dtlStartRow` dopo il codice HTML per riavviare la formattazione del modulo dettagli standard. Viene avviata una seconda griglia i cui campi non sono necessariamente allineati a quelli della prima. Questa tecnica è usata in ogni scheda Notebook.
- Se si desidera inserire un elemento personalizzato alla fine di una riga, è possibile usare la funzione `detailWriteRow()` per scrivere il contenuto di una riga senza chiuderla. È possibile vedere un esempio di questa tecnica nel codice che genera il pulsante "24 Hour" in `detail_cr.html` e `detail_iss.html`.
- Se si desidera specificare esplicitamente il contenuto di un elemento in un riga senza chiudere la tabella che definisce la griglia, è possibile usare la funzione `detailRowHdr()` per specificare il testo dell'intestazione e la funzione `detailSetRowData()` per specificare il testo dei dati. È possibile vedere un esempio di questa tecnica nel codice che genera il campo timer in `detail_cr.html` e `detail_iss.html`.

- Se si fornisce una funzione per convalidare il valore di un campo (normalmente in un gestore eventi) e si desidera che i risultati vengano riportati durante la convalida del browser (in modo che un campo errato venga evidenziato con un bordo rosso e un messaggio di errore venga visualizzato su una striscia gialla nella parte superiore del modulo), usare la funzione `detailReportValidation()`. È possibile vederne un esempio nella funzione `validate_duration()` utilizzata per convalidare i campi di durata in `xx_candp_tab.html`. La funzione `validate_duration()` si trova nel file `val_type.js`.
- Se si desidera esaminare l'HTML generato per un modulo dettagli, è possibile usare le funzioni `docWrite()` e `docWriteLn()` al posto delle funzioni standard `document.write()` e `document.writeLn()`. Quindi, se si richiama la funzione `holdHTMLText()` in un punto qualsiasi nella sezione `<HEAD>` del modulo, CA Service Desk Manager visualizza un modulo di debugging contenente un'area di testo con tutto l'HTML generato per il modulo, che è possibile esaminare, copiare e incollare in uno strumento di convalida.

Mentre si articolano le modifiche, tenere presente che il modulo dettagli di combinazione viene visualizzato sia in una vista di sola lettura che in una di modifica. Se le personalizzazioni sono specifiche dell'una o dell'altra vista, è possibile eseguire il test della vista corrente in uno di questi due modi:

- In JavaScript, `expression _dtl.edit` è `true` nella vista di modifica e `false` in quella di sola lettura.

- In JavaScript o HTML aperto, le istruzioni:

```
<PDM_IF "$prop.form_name_3" == "edit">
```

(codice usato solo nella vista di modifica)

```
</PDM_IF>
```

or

```
<PDM_IF "$prop.form_name_3" == "ro">
```

(codice usato solo nella vista di sola lettura)

```
</PDM_IF>
```

possono essere usate per racchiudere tra parentesi il codice destinato solo alla vista di modifica o di sola lettura, rispettivamente.

detailEndTable()

Questa funzione chiude la tabella HTML che definisce la disposizione degli elementi del modulo dettagli in una griglia. Non dispone di argomenti.

È possibile avviare una nuova griglia con la macro `dtlStartRow()`. Tuttavia, gli elementi in una nuova griglia non sono necessariamente allineati a quelli della griglia precedente.

detailNextID([colspan,][lastelement])

Questa funzione restituisce una stringa nel formato:

```
" ID=df_nn_nn TABINDEX=n onFocus=funz onBlur=funz"
```

Con l'inserimento di questa stringa in un elemento HTML, l'elemento segue le convenzioni della navigazione senza mouse di CA Service Desk Manager, comprese la possibilità di accedere usando i tasti con le frecce e l'evidenziazione in giallo chiaro della zona su cui si passa. La stringa restituita inizia con uno spazio e termina senza spazio.

colspan

Specifica il numero di colonne nella griglia occupate dall'elemento. Questo argomento è opzionale; se non viene specificato, l'impostazione predefinita è uno. Se omesso, si presuppone che l'elemento occupi una colonna della griglia. Ciò influisce sul comportamento dei tasti con le frecce. L'argomento *colspan* può essere omesso anche se si specifica l'argomento *lastelement*.

lastelement

Un valore booleano che specifica se l'elemento per il quale deve essere generato l'ID è l'ultimo della riga. Se omesso, si presuppone che l'elemento sia seguito da altri elementi. Ciò influisce sul comportamento dei tasti con le frecce.

detailNextLinkID()

Questa funzione restituisce una stringa nel formato:

```
" ID=dflink_nn_nn TABINDEX=0 onFocus=funz onBlur=funz"
```

Con l'inserimento di questa stringa in un elemento HTML che definisce un elemento collegamento, l'elemento segue le convenzioni della navigazione senza mouse di CA Service Desk Manager, comprese la possibilità di accedere usando i tasti con le frecce e l'evidenziazione in giallo chiaro della zona su cui si passa. La stringa restituita inizia con uno spazio e termina senza spazio.

Questa funzione non dispone di argomenti.

detailReportValidation(field, has_error, emsg)

Questa funzione restituisce il risultato della convalida esterna di un campo. Se la convalida non è riuscita, il campo viene evidenziato con un bordo rosso e il messaggio di errore specificato viene visualizzato su una striscia gialla nella parte superiore del modulo. L'utente non potrà salvare il record finché una chiamata successiva di detailReportValidation() non indicherà che il campo è privo di errori.

La funzione detailReportValidation() è valida solo per i campi registrati per una convalida del browser. Tutti i campi creati con le macro del modulo dettagli vengono registrati automaticamente per la convalida. Per registrare altri campi, usare la funzione detailSetValidateFunction().

campo

(Richiesto) Specifica l'oggetto elemento del modulo contenente il campo. Il modo più facile per ottenerlo è passare questo argomento al gestore eventi che esegue la convalida. Un altro modo consiste nell'usare la funzione standard JavaScript document.getElementById().

has_error

(Richiesto) Un valore booleano o intero che specifica se il campo è errato. L'impostazione di un campo errato impedisce all'utente di salvare il record, fa sì che il campo venga evidenziato con un bordo rosso e inserisce il messaggio di errore specificato come terzo argomento in una striscia gialla nella parte superiore del modulo. L'impostazione di un campo come senza errori annulla questi cambiamenti.

emsg

Una stringa di testo che specifica il messaggio da visualizzare sulla striscia gialla nella parte superiore del modulo dettagli quando è impostato il flag *has_error*. Questo argomento è obbligatorio se è impostato *has_error*.

detailSetValidate(hdrtext, is_required, maxsize)

Questa funzione specifica che il campo creato più di recente con un ID fornito da detailNextID() è soggetto alla convalida del browser. La convalida dei campi obbligatori e dei campi con dimensione massima è automatica. È possibile usare altri strumenti di convalida tramite le funzioni JavaScript o i gestori eventi che richiamano la funzione detailReportValidation().

È necessario richiamare la funzione detailSetValidate() solo per i campi dei moduli che sono stati definiti personalmente, il cui ID è stato creato da detailNextID(). La funzione detailSetValidate() deve essere richiamata subito dopo aver creato un campo da convalidare. Non è necessario (e produrrebbe risultati imprevisti) richiamare detailSetValidate() per i campi creati dalle macro del modulo dettagli.

hdrtext

(Richiesto) Specifica una stringa usata per identificare il campo nei messaggi di errore.

is_required

(Richiesto) Un valore booleano o intero che specifica se il campo è obbligatorio. CA Service Desk Manager verifica automaticamente che vengano forniti tutti i campi obbligatori ogni volta che l'utente tenta di salvare un record.

maxsize

Un numero intero che specifica la lunghezza massima dei dati per il campo. CA Service Desk Manager verifica automaticamente che tutti i campi con un valore *maxsize* siano della lunghezza consentita ogni volta che l'utente tenta di salvare un record. Questo argomento è obbligatorio. Per eliminare la convalida di *maxsize*, specificare 0.

detailRowHdr(*hdrtext*, *colspan*, *is_required*)

Questa funzione memorizza il testo per l'elemento intestazione (TH) di una voce nella griglia. Il testo non viene realmente scritto nel modulo finché non viene richiamata una funzione *detailWriteRow()* o la macro *dtlStartRow*.

hdrtext

Specifica il testo nell'elemento intestazione. Questo argomento è obbligatorio.

colspan

Specifica il numero di colonne nella griglia occupate dall'elemento. Questo argomento è opzionale; se non viene specificato, l'impostazione predefinita è uno. Se omesso, si presuppone che l'elemento occupi una colonna della griglia. Ciò influisce sul comportamento dei tasti con le frecce. L'argomento *colspan* deve essere specificato se si specifica l'argomento *is_required*.

is_required

Specifica se *hdrtext* deve essere visualizzato nello stile corrispondente a un campo obbligatorio. Questo argomento può essere un valore booleano, un numero o una stringa. Un numero o una stringa vengono interpretati come false se uguali a zero, altrimenti come true. Questo argomento è opzionale; se omesso, lo stile di *hdrtext* è quello di un campo non obbligatorio.

detailSetRowData(*text*)

Questa funzione memorizza il testo HTML per l'elemento dati (TD) di una voce nella griglia. Il testo non viene realmente scritto nel modulo finché non viene richiamata una funzione *detailWriteRow()* o la macro *dtlStartRow*. L'unico argomento è il testo HTML dell'elemento da memorizzare.

detailWriteRow()

Questa funzione scrive l'HTML memorizzato per la riga corrente. Vengono create due righe di tabella HTML, una per gli elementi intestazione (TH) e una per gli elementi dati (TD). Questa funzione, inoltre, scrive il tag [assign the value for TD in your book] che inizia un nuovo elemento dati. Il tag TD viene chiuso automaticamente dalla macro `dtlStartRow`, così non è necessario (e non sarebbe corretto) fornire i tag [assign the value for TD in your book] nel testo HTML che segue `detailWriteRow()`. Questa funzione non dispone di argomenti.

Analisi dei moduli elenco

Di seguito si forniscono informazioni di base sugli elementi interni che costituiscono i moduli elenco CA Service Desk Manager. Si raccomanda di utilizzare Screen Painter Web Design View per modificare questi moduli.

I moduli elenco CA Service Desk Manager sono definiti tramite le macro seguenti (richiamate dal tag `PDM_MACRO`):

IsStart

Inizia un elenco

IsCol

Definisce una colonna in un elenco

IsWrite

Inserisce il testo nella parte `pdm_list` di un elenco

IsEnd

Termina un elenco

Il formato generale di un elenco usando queste macro è:

```
<pdm_macro name=IsStart>
<pdm_macro name=IsCol hdr=hdr1 attr=attr1>
<pdm_macro name=IsCol hdr=hdr1 attr=attr1>
<pdm_macro name=IsEnd>
```

Questo genera un testo nell'HTML di output simile al seguente:

```
var rs = new Resultset();           From IsStart
rs.startList(); From IsStart
rs.header("hdr1"); From IsCol
rs.setData("attr1","options"); From IsCol
rs.header("hdr2"); From IsCol
rs.setData("attr2","options"); From IsCol
<PDM_LIST SOURCE=list> From IsEnd
rs.data(attr1) From IsCol/IsEnd
rs.data(attr2) From IsCol/IsEnd
</PDM_LIST> From IsEnd
```

Nota: sono presenti due diverse sezioni nell'elenco output: la sezione setup prima del tag <PDM_LIST>, e l'elenco effettivo tra i tag <PDM_LIST> e </PDM_LIST>. La macro IsCol usa le variabili di preelaborazione e il tag <PDM_SET> per generare i dati di entrambe le sezioni dell'elenco. L'intera sezione elenco è creata da un tag <PDM_EVAL> generato dalla macro IsEnd.

Per inserire personalizzazioni in JavaScript nella sezione di configurazione dell'elenco, è sufficiente includere il codice dove necessario. Per inserire codice personalizzato nella sezione elenco, usare la macro IsWrite.

Ulteriori informazioni:

[Modifica di moduli elenco e dettagli nella vista Progetto](#) (a pagina 303)

Macro IsWrite

La macro IsWrite specifica il testo per la sezione elenco (la parte compresa tra i tag <pdm_list> e </pdm_list>) in un elenco. Il testo specificato per l'argomento text di questa macro è rinviato e non viene scritto nell'HTML di output finché non viene eseguita la macro IsEnd.

IsWrite [entrambi=no|sì]

text="xxx"

both

Specifica che l'operando text deve essere scritto sia subito nell'HTML di output che nel buffer del testo rinviato. Ciò può essere utile per generare JavaScript che ignori, in determinate condizioni, sia le informazioni di configurazione che quelle di elenco generate da una successiva macro IsCol. Opzionale; l'impostazione predefinita è no.

testo

Specifica il testo generato da questa macro. Il testo specificato viene rinviato finché non viene eseguita la macro IsEnd.

Spesso è preferibile includere i tag PDM e i riferimenti alle variabili del modulo nell'output di testo generato da una macro IsWrite. Per impedire che vengano interpretati dal motore Web durante l'analisi della macro IsWrite, applicare queste regole di sintassi:

- Se la macro IsWrite genera un pdm_tag, omettere i delimitatori "<" e ">" del tag. Ad esempio, per inserire un'istruzione <pdm_else> nella sezione elenco, scrivere:

```
<PDM_MACRO NAME=IsWrite text="pdm_else">
```

Il motore Web inserisce automaticamente "<" e ">" prima di generare il testo quando rileva che i primi quattro caratteri sono "pdm_" (o "PDM_").

- Se la macro IsWrite genera un riferimento a una variabile del modulo, scrivere un carattere @ al posto del carattere \$ che designa la variabile. Ad esempio, per generare un riferimento alla variabile elenco \$list.persistent_id, scrivere:

```
<PDM_MACRO NAME=IsWrite text="@list.persistent_id">
```

Il motore Web converte automaticamente il carattere "@" in "\$" prima di generare il testo. Per generare un segno letterale @, farlo precedere da una barra rovesciata.

Personalizzazione di Modifica in elenco

Diversi moduli elenco, come gli elenchi delle richieste e delle questioni, includono un pulsante Modifica in elenco. Quando questo pulsante è disponibile e un set di risultati viene visualizzato, l'utente può fare clic sul pulsante per sostituire il filtro di ricerca con un piccolo modulo di modifica. Il modulo di modifica consente all'utente di aggiornare i record direttamente sul modulo elenco. L'utente può anche aggiornare tutto quanto è selezionato nell'elenco inserendo i nuovi dati nel modulo di modifica e facendo clic su Modifica tutto.

Durante la modifica dei dati dell'elenco non c'è comunicazione con il server, finché l'utente non fa clic su Salva. Quanto l'utente fa clic su Salva, tutti gli aggiornamenti (evidenziati in giallo sul modulo) vengono inviati al server che applica tutti i cambiamenti in un'unica operazione, restituendo un messaggio di stato e visualizzando di nuovo l'elenco.

È possibile personalizzare questa funzione controllando se il pulsante Modifica in elenco è disponibile in un particolare modulo e controllando i campi riportati nel modulo di modifica visualizzato quando l'utente fa clic su Modifica in elenco.

Per inserire un pulsante Modifica in elenco in un modulo elenco, includere l'istruzione seguente in un punto qualsiasi della sezione <HEAD> del modulo:

```
<SCRIPT LANGUAGE="JavaScript" SRC=$CAisd/CAisd/list_edit.js></SCRIPT>
```

L'aggiunta di questa istruzione è sufficiente a inserire il pulsante nel modulo. Tuttavia, il pulsante è disattivato a meno che nel modulo non siano incluse anche le istruzioni JavaScript che specificano il contenuto del modulo di modifica. Queste istruzioni devono essere inserite subito prima della specifica del set di risultati e devono avere il formato seguente:

Istruzioni	Commenti
startListEdit(_search_filter);	Specificarla esattamente come indicato

Istruzioni	Commenti
<code>listEditStartRow();</code>	Specificarla esattamente come indicato
<code>listEditField("attr"[, "hdr"]);</code>	Specificare zero o un numero maggiore
<code>listEditReadonly("attr"[, "hdr"]);</code>	Specificare zero o un numero maggiore
<code>endListEdit();</code>	Specificarla esattamente come indicato

L'istruzione `endListEdit()` deve essere seguita dall'istruzione `ResultSet()` che inizia il set di risultati. Specificare i campi e la relativa sequenza nel modulo di modifica scrivendo una o più istruzioni `listEditReadonly()` o `listEditField()`.

`startListEdit( _search_filter );`

Questa istruzione inizia il modulo di modifica elenco. Deve essere scritta esattamente come indicato.

`listEditStartRow();`

Questa istruzione inizia una nuova riga di campi sul modulo di modifica elenco. Deve essere scritta esattamente come indicato. È necessario inserire un'istruzione `listEditStartRow()` subito dopo l'istruzione `startListEdit()`. È possibile includere altre istruzioni `listEditStartRow()` tra le istruzioni `listEditField()` e `listEditReadonly()` che specificano i campi nel modulo.

listEditField(attr_name[,hdr]);

Questa istruzione specifica un attributo da includere nel modulo di modifica elenco.

attr_name

Consente di specificare il nome dell'attributo da includere nel modulo di modifica (punti compresi, se appropriato). Tutti gli attributi specificati per un modulo di modifica elenco devono essere presenti anche nel set di risultati. L'argomento *attr_name* specificato deve essere identico a quello specificato nell'istruzione `rs.showData()` o `rs.showDataWithLink()` per aggiungere l'attributo al set di risultati.

L'attributo viene visualizzato sul modulo di modifica nello stesso formato in cui è visualizzato nel filtro di ricerca. Se l'attributo non è presente nel filtro di ricerca, viene modificato in una casella di testo a 20 caratteri.

attr_name è un argomento obbligatorio.

hdr

Consente di specificare il testo dell'intestazione nel campo del modulo di modifica. Questo argomento è opzionale; se omissso, il testo dell'intestazione viene preso dal filtro di ricerca. Se *hdr* viene omissso e l'attributo non è presente nella voce del filtro di ricerca per *attr_name*, per impostazione predefinita come testo dell'intestazione viene utilizzato il nome dell'attributo compreso tra punti interrogativi.

listEditReadonly(attr_name[,hdr]);

Questa istruzione specifica un attributo non modificabile da includere nel modulo di modifica elenco. Gli argomenti hanno lo stesso significato di quelli di `listEditField()`.

endListEdit();

Questa istruzione termina il modulo di modifica elenco. Deve essere scritta esattamente come indicato.

Integrazione con le proprie pagine Web

Questa sezione descrive come integrare le funzionalità dell'interfaccia Web CA Service Desk Manager con le proprie pagine Web in modo da presentare un'interfaccia coerente agli utenti.

Nota: il motore Web, cioè il file eseguibile che agisce da gateway tra il server Web e il server CA Service Desk Manager, consente più connessioni di un determinato utente contemporaneamente. Più di un frame alla volta può avere una connessione aperta con il processo del motore Web CA Service Desk Manager.

Le interfacce Web possono essere integrate nei modi seguenti:

- Creando collegamenti da qualsiasi pagina Web alla pagina Web CA Service Desk Manager appropriata, senza dover passare per la pagina dei menu dell'interfaccia Web.
- Aggiungendo moduli HTML alle pagine Web che raccolgono l'input ed eseguono direttamente le operazioni supportate, senza dover visualizzare le pagine di immissione dei dati Web CA Service Desk Manager.
- Creando gruppi di moduli Web che possono essere usati per associare i moduli HTML basati sul Web agli utenti tramite il rispettivo tipo di accesso. Analogamente ai gruppi di moduli usati dal client di amministrazione, i gruppi di moduli Web possono essere usati per personalizzare le proprie pagine HTML.

Ulteriori informazioni:

[Operazioni supportate](#) (a pagina 350)

Collegamento alle funzioni CA Service Desk Manager

È possibile collegarsi direttamente alle principali funzioni CA Service Desk Manager senza dover visualizzare la pagina principale. Normalmente questo è possibile accedendo al popup della nuova finestra che contiene le informazioni di CA Service Desk Manager. Oppure è possibile anche sostituire la pagina Web con la pagina di CA Service Desk Manager.

In entrambi i casi, CA Service Desk Manager visualizza la pagina richiesta allo stesso modo in cui la vede l'utente in una normale sessione ma senza la pagina principale e il segnapunti. Un analista può visualizzare la pagina principale e il segnapunti selezionando Ripristina segnapunti dal menu File, disponibile solo sulle pagine visualizzate ignorando la pagina principale.

Per creare un collegamento che ignori la pagina principale, specificare un URL in questo formato:

`http://hostname[:porta]/CAisd/pdmweb.exe?OP=operation+var=valore+...`

In questo URL di esempio, *hostname* è la macchina server Web; *porta* è il numero della porta (di solito 8080) necessario solo se si usa Tomcat come server http; *operation* è una delle operazioni supportate e *var=value* è una o più delle variabili consentite con l'operazione.

Ad esempio, un collegamento che carica il modulo per creare una nuova richiesta può essere specificato in questo modo:

`<A HREF=http://hostname/CAisd/pdmweb.exe?OP=CREATE_NEW+FACTORY=cr>Definisci richiesta</A>`

Ulteriori informazioni:

[Esempi di collegamenti](#) (a pagina 358)

Pubblicazione dei moduli in CA Service Desk Manager

È possibile accedere alle funzionalità CA Service Desk Manager anche aggiungendo moduli HTML alle pagine Web che fanno riferimento alle operazioni supportate. Se il modulo viene inviato con informazioni sufficienti a eseguire l'operazione, come la creazione di una richiesta, l'operazione viene eseguita senza visualizzare un modulo per raccogliere ulteriore input.

Quando si aggiunge un modulo HTML alla pagina Web:

- L'ACTION del modulo è l'URL di pdmweb.exe.
- Il METHOD è POST.
- Il nome del pulsante SUBMIT deve essere una delle operazioni supportate o deve essere disponibile un campo nascosto chiamato OP il cui valore è una delle operazioni supportate.

Ad esempio, per creare un modulo HTML che carica la pagina per creare una nuova richiesta, specificare il codice seguente:

```
<FORM ACTION=/CAisdCAisd/pdmweb.exe METHOD=POST>
<INPUT type=HIDDEN NAME=FACTORY VALUE=iss>
.
.
.
<INPUT type=SUBMIT NAME=CREATE_NEW VALUE=" OK ">
</FORM>
```

Personalizzazione JavaScript

L'interfaccia Web CA Service Desk Manager usa intensivamente il linguaggio JavaScript e include numerosi file JavaScript nella directory /CAisd/scripts. Se si decide di personalizzare uno di questi file script, inserire la versione modificata in /CAisd/sitemods/scripts, come già descritto in [Directory usate dal server HTTP](#) (a pagina 366).

Per motivi di prestazioni, i file JavaScript distribuiti nella directory /CAisd/scripts sono compressi, privi dei commenti e degli spazi inutili. Tale compressione può renderne difficoltosa la lettura. È possibile trovare versioni non compresse di tutti i file JavaScript in una delle directory seguenti:

- (UNIX) \$NX_ROOT/sdk/scripts
- (Windows) \$NX_ROOT/sdk/scripts

Se possibile, evitare di creare versioni personalizzate dei file JavaScript per intero, dato che ogni file contiene un certo numero di funzioni e magari si è interessati a modificarne solo una. In molti casi, è possibile ignorare singole funzioni inserendo una versione modificata nel file JavaScript `sitemods.js`. Si consiglia caldamente di praticare questo approccio alla modifica del JavaScript.

`sitemods.js`

In CA Service Desk Manager è disponibile un file di esempio *sitemods.js*. Tutti i file HTML distribuiti includono questo file alla fine della sezione `<head>` in modo che sia l'ultimo file JavaScript a essere caricato. Essendo l'ultimo file, tutte le funzioni in esso definite sostituiscono le funzioni aventi lo stesso nome e presenti nelle parti precedenti. Ciò consente di fornire una propria versione di una funzione JavaScript senza modificare direttamente il codice distribuito.

Questo approccio non funziona per funzioni richiamate al caricamento nella sezione `<head>`, come quelle in `menubar.js` e `ahdmenus.js`.

Tuttavia, è possibile personalizzare la maggior parte delle funzioni JavaScript completando i seguenti passaggi:

1. Inserire una versione modificata della funzione in `sitemods.js`.
2. Memorizzare la copia aggiornata di `sitemods.js` in `CAisd/site/mods/www/wwwroot/scripts`.

Ulteriori informazioni:

[Modifica delle barre dei menu](#) (a pagina 309)

Modifica dei menu di scelta rapida

Numerosi moduli in CA Service Desk Manager usano menu di scelta rapida a cui si accede facendo clic con il pulsante destro del mouse su un oggetto. Usando Screen Painter Web, è possibile modificare i menù a scelta rapida per aggiungere, rimuovere o modificare le voci.

Nota: per ulteriori informazioni circa l'aggiunta di voci di menù, consultare la *Guida Screen Painter Web*.

Aggiornamento e creazione degli ordini di cambiamento come dipendente

Per impostazione predefinita, l'interfaccia Web per i dipendenti consente solo di visualizzare gli ordini di cambiamento. Attenersi alla procedura seguente per consentire la creazione e l'aggiornamento degli ordini di cambiamento ai dipendenti:

1. Accedere al Web come amministratore, quindi selezionare la scheda Amministrazione.
2. Selezionare Tipo di accesso dal menu Protezione.
Viene visualizzata la finestra Elenco tipi accesso.
3. Selezionare il collegamento Dipendente per visualizzare la finestra Dettagli tipo accesso dipendente.
4. Impostare Ordini di cambiamento su "modifica", nella scheda Accesso funzioni, quindi salvare.
5. Fare clic sul pulsante Indietro per tornare alla scheda Amministrazione, quindi selezionare Partizioni dati, Elenco partizioni dati.
6. Fare clic su Dipendente per visualizzare la finestra Dettagli partizioni dati. Nella sezione Elenco vincoli della colonna Tipo verificare le tabelle Change_Request seguenti:
 - Aggiornamento preliminare
 - Crea
7. Per ogni tabella che si desidera modificare, fare clic sul nome della tabella per visualizzare la finestra Dettagli vincolo partizione dati della tabella.
8. Fare clic sul pulsante Modifica.
9. Modificare i vincoli seguendo la procedura descritta di seguito:
change "id = 1" to "affected_contact = @root.id".
10. Fare clic su Salva.

Quando si accede all'interfaccia Web come utente dipendente, viene visualizzato il collegamento *Crea ordine di cambiamento*.

Aggiungere un collegamento "Ordini di cambiamento chiusi" al contatore dipendente.

È possibile aggiungere un'opzione nodo Cambiamenti chiusi al contatore dell'interfaccia Web Dipendente.

Per aggiungere un nodo Cambiamenti chiusi

1. Accedere come Amministratore.
2. Fare clic sulla scheda Service Desk.

3. Selezionare File, Personalizza contatore.
Compare la finestra di dialogo Personalizza contatore.
4. Fare click sull'opzione Ruolo e selezionare Dipendente nell'elenco a discesa.
5. Sotto Aggiungi nuovo nodo, fare click sul collegamento Query memorizzata del nodo.
Viene visualizzato l'Elenco query memorizzate.
6. Cercare e selezionare Cambiamenti chiusi dall'Elenco query memorizzate. Questo è l'aspetto tipico del codice CHGUBIN7.
7. Per indicare l'ubicazione del nuovo nodo, selezionare un elemento nella struttura segnapunti a sinistra.
8. Fare clic su Aggiungi nuovo nodo.
Il nuovo nodo, Cambiamenti chiusi, viene aggiunto alla struttura del contatore.
9. Fare clic su Fine.

Download degli allegati

Quando si scarica un allegato in CA Service Desk Manager, l'allegato viene visualizzato automaticamente nella finestra del browser senza chiedere una risposta. Questa operazione può essere pericolosa se l'allegato è infetto da un virus.

Con CA Service Desk Manager è possibile forzare la visualizzazione di una finestra di dialogo di salvataggio che chieda se si desidera salvare l'allegato sul disco o aprirlo. Questo può essere un metodo sicuro in quanto si può salvare l'allegato sul disco e analizzarlo prima di aprirlo effettivamente. È possibile anche forzare la visualizzazione della finestra di dialogo di salvataggio solo per determinati tipi di allegati.

È possibile forzare la comparsa di una finestra di dialogo di salvataggio mediante il file di configurazione servlet web.xml. Il file web.xml si trova nei percorsi seguenti:

Windows: \$NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml

Linux: \$NX_ROOT è "/opt/CAisd"

Personalizzazione della memorizzazione dei dati del registro eventi

La variabile di ambiente di sistema `@NX_EVENT_LOG_EXCLUDE`, che viene impostata nel file `NX.env` e richiede un riavvio dei servizi CA Service Desk Manager, permette di controllare la quantità di dati memorizzati nel registro eventi (tabella `event_log`). Questa variabile permette di memorizzare solo gli eventi di cui si vuole mantenere traccia, realizzare report e utilizzare come parte dell'attività recente che può essere avviata come bottone nella pagina Profilo rapido.

In questa variabile, una virgola separa le voci elenco (per esempio, `@NX_EVENT_LOG_EXCLUDE = FAQ,KD_OPEN`). Per esempio, se si utilizzano gli eventi LOGIN, LOGOUT dalla seguente tabella (`@NX_EVENT_LOG_EXCLUDE` valore di LOGIN, LOGOUT), il prodotto non registra gli eventi di accesso e disconnessione.

Fare riferimento alle seguenti informazioni per personalizzare i dati da memorizzare nel registro eventi mediante questa variabile.

Evento	Enumerazione	Pubblicato da	Set	Commenti
LOGIN	1	CA Service Desk Manager		Specifica che l'utente effettua l'accesso nel sistema.
LOGOUT	2	CA Service Desk Manager	numdata1	Specifica che l'utente si disconnette, dove numdata1=motivo disconnessione: 0 —normal 1 —timeout 2 —abnormal
CR_CREATE	3	CA Service Desk Manager	sd_obj_type, sd_obj_id, kd, numdata1	Indica che l'utente crea una richiesta, dove numdata1=id dell'utente finale interessato.
ISS_CREATE	-4	CA Service Desk Manager	sd_obj_type, sd_obj_id, kd, numdata1	Indica che l'utente crea un ordine di cambiamento, dove numdata1=id dell'utente finale interessato.
CHG_CREATE	5	CA Service Desk Manager	sd_obj_type, sd_obj_id, kd, numdata1	Indica che l'utente crea una questione, dove numdata1=id dell'utente finale interessato.
EMAIL	/6	Gestione delle	kd	Specifica che l'analista invia un documento tramite posta

Evento	Enumerazione	Pubblicato da	Set	Commenti
		informazioni		elettronica.
LINK	7	Gestione delle informazioni	kd, sd_obj_type, sd_obj_id	Indica che l'utente accetta una soluzione e la collega a un ticket.
ANNULLA COLLEGAMENTO	8	CA Service Desk Manager	sd_id, sd_obj_type, sd_obj_id	Specifica che l'utente annulla il collegamento di una soluzione da un ticket.
SEARCH	9	Gestione delle informazioni	numdata1,	Indica che l'utente esegue ricerche nella Knowledge Base, dove numdata1= CI_ASKED_QUES id.
FAQ	10	Gestione delle informazioni	numdata1	Indica una ricerca FAQ, dove numdata1= O_INDEXES id (categoria).
DT_NAVIGATE	11	Gestione delle informazioni	kd, numdata1, textdata1	Indica che l'utente esplora una struttura decisionale, dove numdata1= ES_NODES ID textdata1=percorso.
KD_BOOKMARK	12	Gestione delle informazioni	kd	Indica che l'utente aggiunge un segnalibro a un documento di conoscenza.
KD_COMMENT	13	Gestione delle informazioni	kd, numdata1	Indica che l'utente aggiunge un commento a un documento della conoscenza, dove numdata1= id O_COMMENTS.
KD_CREATE	14	Gestione delle informazioni	sd_ob_type, sd_obj_id, kd	Specifica che un utente crea un nuovo documento. Gli ID CA Service Desk Manager sono utilizzati quando un documento di conoscenza viene creato utilizzando Invio conoscenza da una richiesta o da una questione.
KD_OPEN	15	Gestione delle informazioni	kd, numdata1	Indica che l'utente apre un documento di conoscenza, dove numdata1=BU_TRANS ID.
KD_RATE	16	Gestione delle informazioni		Indica che l'utente classifica un documento di conoscenza, dove numdata1=BU_TRANS ID.
KD_NEW	17	Gestione delle	numdata1	Specifica che un utente seleziona

Evento	Enumerazione	Pubblicato da	Set	Commenti
		informazioni		la cartella Nuovi documenti nella scheda Conoscenza.
NX_ATTACH_AUDIT_TO_NEW_TICKET	18	CA Service Desk Manager		Quando un utente apre un nuovo ticket, tutti gli eventi per la sessione attuale compaiono di default nella scheda Registro eventi del ticket. 0—Solo gli eventi rilevanti per il ticket compaiono nella scheda Registro eventi. 1—Tutti gli eventi per la sessione corrente compaiono nella scheda Registro eventi del ticket .
TICK_OPEN	19	CA Service Desk Manager		Indica che il ticket è stato visualizzato.
TICK_SEARCH	20	CA Service Desk Manager		Indica che l'utente ha cercato i ticket e collega il numero di ricerche.
KD_PRNT	21	Gestione delle informazioni	kd	Indica che è stato stampato un documento della conoscenza.

Personalizzazione dei report di CA Business Intelligence

È possibile personalizzare i report di CA Business Intelligence, a cominciare dal punto dopo che i campi e le tabelle sono stati definiti nello schema CA Service Desk Manager.

Nota: per informazioni su come funzionano le modifiche allo schema, consultare la [Panoramica di modifica progettazione schema](#) (a pagina 283).

Prima di iniziare, assicurarsi di aver realizzato le seguenti operazioni:

- Installazione di CA Business Intelligence e configurazione di CA Business Intelligence in modo che funzioni correttamente con CA Service Desk Manager.
- Siano state stabilite le autorizzazioni utente, i ruoli, le opzioni di autenticazione e le partizioni dati per l'ambiente di reporting.

Nota: per informazioni sulla configurazione della protezione CA Business Intelligence, vedere la *Guida all'amministrazione*.

Infrastruttura di CA Business Intelligence

CA Business Intelligence (CA BI) è un'infrastruttura di reporting aziendale che consente di creare, mantenere, memorizzare, pianificare e distribuire i report per gli utenti e i ruoli di CA Service Desk Manager. BusinessObjects Enterprise XI, Release 2 e i suoi strumenti associati, insieme a BusinessObjects Crystal Reports XI sono la struttura portante dell'architettura. Gli strumenti BusinessObjects Enterprise sono contenuti all'interno di un pacchetto CA Service Desk Manager, che unisce gli elementi essenziali di reporting di CA Service Desk Manager in una struttura di business intelligence leader del settore.

Nota: sebbene i Crystal Reports siano forniti come componente primario di CA BI, lo strumento di creazione e manutenzione dei report, Crystal Reports XI, non è fornito. Crystal Reports XI è un prodotto distribuito sotto un'altra licenza e può essere acquistato da BusinessObjects e utilizzato insieme a CA BI.

Componenti del reporting

Di seguito si elencano i componenti primari inclusi nell'infrastruttura di CA Business Intelligence:

- Database **CA Service Desk Manager** / Domsrvr / Driver ODBC—I dati dei report vengono memorizzati in un database CA Service Desk Manager SQL Server o Oracle. Le applicazioni di reporting di BusinessObjects (Crystal Reports e Web Intelligence) accedono al database utilizzando un driver ODBC che li collega direttamente al motore oggetti di CA Service Desk Manager (domsrvr). Tutta la sicurezza CA Service Desk Manager, incluse le restrizioni tenancy e di partizione dati, viene applicata automaticamente ai report.
- **Central Management Server**—CMS è il repository centrale che memorizza tutti gli oggetti utilizzati in ciascun processo di reporting.

- **Central Management Console**— CMC è lo strumento di amministrazione principale per BusinessObjects. Fornisce l'accesso a tutte le funzioni di amministrazione di BusinessObjects. Utilizzando il CMC, è possibile distribuire report e assegnare accesso utente e autorizzazioni di cartella per InfoView.
- **BusinessObjects Universe**—L'universo fornisce una rappresentazione di business di un data warehouse o di un database transazionale. Descrive le classi (tabelle) e gli oggetti (colonne) utilizzati nei report. L'universo CA Service Desk Manager viene installato e configurato durante l'installazione. Al completamento dell'installazione, il collegamento dell'universo viene assegnato a diversi gruppi e utenti in CA Service Desk Manager.
 - **Designer**—È uno strumento di BusinessObjects Enterprise che consente di modificare l'universo CA Service Desk Manager, che è un meta layer tra lo schema CA Service Desk Manager e gli strumenti di reporting di BusinessObjects. La procedura guidata di importazione/esportazione facilita la compilazione o l'estrazione dell'oggetto all'interno del CMS.
- **Report predefiniti**—Sono report CA Service Desk Manager e Gestione delle informazioni basati sul Web e sviluppati con Web Intelligence o Crystal Reports. I report possono essere utilizzati come modelli per definire report specifici in base ai siti.
- **InfoView**—è un'interfaccia Web di BusinessObjects che consente agli utenti autorizzati CA Service Desk Manager di interagire con i report predefiniti basati sul Web, visualizzando, eseguendo e pianificando i tipi di report tra cui WebI e Crystal Reports. I report sono contenuti in cartelle nella sezione pubblica di InfoView.
- **Report ad hoc**—Vengono creati e gestiti da InfoView utilizzando un'interfaccia Web Intelligence basata su plugin. Questo strumento è pensato per utenti che desiderano creare report di base senza scrivere query.

Ambiente di sviluppo

L'aggiornamento dell'infrastruttura CA BI con i cambiamenti dello schema CA Service Desk Manager è una funzione amministrativa. Un amministratore che promuove uno schema modificato nei report deve impostare l'ambiente, a parte dal loro ambiente di produzione.

Alcuni degli strumenti usati da BI richiedono un'architettura basata su Windows. Questo significa che le installazioni di Linux/UNIX devono configurare CA BI in un computer Windows per interagire con l'installazione CA BI in ambiente di produzione Linux/UNIX. Se si stanno utilizzando server Windows in produzione, occorre configurare un computer Windows aggiuntivo per l'ambiente di sviluppo.

Strumenti

L'aggiornamento dell'infrastruttura CA BI con i cambiamenti dello schema CA Service Desk Manager è una funzione amministrativa. Per favorire i cambiamenti dello schema cambiate nei report, occorre includere i seguenti strumenti nell'ambiente di sviluppo:

Business Objects Designer

Questo strumento client completo Windows è installato sul server di produzione di CA BI come parte dell'installazione base di CA BI per Windows. Quando il server di CA BI ha un'architettura non Windows, o quando l'accesso mediante login al server dell'applicazione di CA BI di produzione è sconsigliato, occorre creare un'installazione separata di CA BI su un server Windows (di sviluppo). Un'installazione server di sviluppo di CA BI permette di accedere agli oggetti di produzione di CA BI da remoto, indipendentemente dall'architettura dell'installazione del server di produzione di CA BI.

BusinessObjects Web Intelligence

Questo strumento di creazione di report mediante interfaccia Web serve per modificare e creare report di Web Intelligence (WebI). È possibile accedere allo strumento WebI mediante l'interfaccia InfoView di BusinessObjects. Le autorizzazioni amministrative degli strumenti WebI e InfoView sono disponibili all'interno di CA BI, utilizzando specificamente lo strumento Console di gestione centralizzata (CMC) di BusinessObjects.

Driver ODBC CA Service Desk Manager

Il driver ODBC di CA Service Desk Manager è fornito insieme all'installazione di CA BI. Questo componente consente ai report WebI e Crystal Reports di accedere ai dati CA Service Desk Manager rafforzando la protezione della partizione dati. Il driver ODBC è installato come parte dell'installazione di base di CA BI sul server di applicazione di CA BI. È anche disponibile come installazione client, in modo che possa essere utilizzato su un computer che non esegue CA BI insieme al client Crystal Reports XI.

Nota: per informazioni sulla definizione della protezione della partizione dati per l'ambiente di reporting, vedere la *Guida all'amministrazione*.

Modalità di creazione di un ambiente di sviluppo

Per creare un ambiente di sviluppo, procedere come segue:

1. Predisporre un server con un sistema operativo Windows supportato.
2. Installazione e configurazione di CA Service Desk Manager.
3. Installare e configurare CA Business Intelligence.

4. Cambiare il nome predefinito di ODBC DSN da casd_XXXXX to casd_YYYYY dove YYYYY è esattamente lo stesso di DSN nell'implementazione di produzione.

Importante indipendentemente dalle proprietà effettive della connessione, il nome DSN nelle implementazioni di sviluppo e produzione deve essere identico.

5. (Facoltativo) Installare e configurare Crystal Reports XI.

Nota: non è necessario installare Crystal Reports sullo stesso computer di CA BI. Crystal Reports può essere installato in un computer diverso, purché il driver ODBC di CA Service Desk Manager è anche installato sul computer con Crystal Reports, e il nome DSN è modificato per essere identico a quello dell'implementazione di produzione, indipendentemente dalle effettive proprietà di connessione. Per ulteriori informazioni sull'installazione di una copia individuale del driver ODBC di CA Service Desk Manager, separata dall'installazione di CA BI, consultare la documentazione del driver ODBC.

6. [Creare la struttura](#) (a pagina 394).

Struttura

Dopo aver reso disponibili gli strumenti nell'ambiente di sviluppo, occorre creare una struttura che consenta di conservare i cambiamenti dello schema attraverso gli aggiornamenti del prodotto.

Importante Non modificare l'universo di sviluppo di CA Service Desk Manager installato per impostazione predefinita con CA BI. In caso contrario, i cambiamenti dello schema potrebbero venire sovrascritte durante i processi di patch e aggiornamento. La modifica dell'universo CA Service Desk Manager potrà alla fine risultare nella perdita dei cambiamenti dello schema all'interno dell'infrastruttura CA BI.

L'universo BusinessObjects è il metalayer che descrive lo schema all'interno dell'infrastruttura CA BI. Invece di modificare l'universo CA fornito, si può creare un universo specifico per il cliente collegato all'universo CA Service Desk Manager. Utilizzando questo approccio, è possibile mantenere i cambiamenti locali dello schema con il minimo sforzo durante il processo di aggiornamento e CA Service Desk Manager sarà in grado di fornire gli aggiornamenti all'universo di base.

I clienti di CA Service Desk Manager a conoscenza della documentazione dell'universo BusinessObjects saranno al corrente di altre procedure documentate disponibili da BusinessObjects che permettono di collegare universi. Il procedimento discusso qui, tuttavia, è l'unico procedimento supportato da CA per mantenere le modifiche del cliente.

L'universo predefinito è denominato "CA Service Desk Manager" ed è memorizzato nella cartella "CA Universes" all'interno della Console di gestione centralizzata (CMC). Questo universo predefinito è l'universo "kernel" in una struttura in cui sono collegati gli universi.

L'universo CA Service Desk Manager può avere un nome qualsiasi a scelta. Il nome sarà mostrato a chi stila i report quando ne stanno creando uno, di conseguenza deve essere un nome significativo. L'universo del cliente è un universo "derivato" in una struttura in cui gli universi sono collegati.

All'interno di questa struttura, è possibile mantenere qualsiasi numero di universi derivati ma soltanto uno serve per mantenere i cambiamenti dello schema. Si possono utilizzare vari universi derivati per facilità di manutenzione o requisiti di sicurezza, ma tali decisioni sono ad esclusiva discrezione delle proprie esigenze di supporto in produzione.

In un ambiente di universo derivato, verificare quanto segue:

- Mantenere la convenzione z_ nel nome per il nome del file universo in tutti gli universi.
- Usare la connessione CA Service Desk Manager, dopodiché salvare l'universo nella cartella CA Universo cliente.
- Non cancellare il collegamento all'universo kernel.

Creazione di una struttura per la promozione dei cambiamenti dello schema in CABI

Per creare una struttura di promozione dei cambiamenti dello schema in CA Business Intelligence

1. Aprire la progettazione di BusinessObjects.
Selezionare File, New dal menu Designer.
Viene visualizzata la finestra di dialogo Parametri universo.
2. Fare clic sulla scheda Definition ed immettere un nome significativo per questo universo nel campo Name.
3. (Facoltativo) Immettere una descrizione nel campo Descrizione.
4. Selezionare CA Service Desk Manager dall'elenco a discesa Connection.
5. Fare clic sul pulsante Add Link nella scheda Links.
Compare la finestra di dialogo Universo a collegamento.

6. Espandere le cartelle Universi di CA e completare i seguenti passaggi:

- a. Aprire il file CA Service Desk.unv. Si chiude la finestra di dialogo Universo a collegamento e compare l'universo CA Service Desk Manager nella scheda Collegamenti.
- b. Fare clic su OK per chiudere la finestra di dialogo Parametri universo.

Il programma può impiegare alcuni minuti ad elaborare il collegamento e a creare l'universo derivato.

7. Dopo la creazione dell'universo derivato, realizzare le seguenti operazioni:

- a. Modificare il(i) parametro(i) seguente(i) in modo appropriato.
 - Selezionare Parameters nel menu File.
 - Fare clic sulla scheda Parameter.
 - Specificare ANSI92 = Sì.
- b. Fare click sulla scheda Controlli e impostare i seguenti campi con un valore adatto alla propria implementazione, dopodiché fare click su OK per salvare i valori e chiudere la finestra di dialogo dei parametri:
 - Dimensioni limite del set risultati
 - Tempo limite di esecuzione
 - Dimensioni limite di oggetti testo lunghi (minimo 4000).
- c. Definire le gerarchie. Notare che le gerarchie di clienti non vengono importate.
 - Selezionare Tools, Hierarchies.
 - Eseguire la selezione multipla di tutte le gerarchie personalizzate, quindi fare clic sul pulsante freccia Add. Tutte le gerarchie vengono spostate al lato destro.

8. Dal menu Designer fare clic su File, Save.

Viene visualizzata la finestra Salva con nome.

9. Nel campo File Name, selezionare un nome file descrittivo, quindi elaborare il nome file con "z_". Per esempio, un universo che si chiama "ACME Anvil Co" può diventare per impostazione predefinita: "ACME_Anvil_Co.unv". Modificare questo nome file in questo modo: "z_ACME_Anvil_Co.unv" prima di salvare.

10. Esportare l'universo derivato nel CMS nel modo seguente:

- a. Selezionare File, Export dal menu Designer.
- b. Dall'elenco a discesa del campo Domain, selezionare <Browse>, quindi individuare e selezionare gli universi dei clienti CA.

- c. Fare click su OK per esportare l'universo al CMS locale

Viene visualizzata la finestra di dialogo Universe Successfully Exported.

A questo punto, esiste la struttura per promuovere i cambiamenti dello schema personalizzato attraverso CA BI.

11. Effettuare l'accesso in BusinessObjects InfoView come amministratore e seguire questi passaggi:

- a. Selezionare Cartelle pubbliche.
- b. Dalla barra degli strumenti di InfoView, fare clic su New, Folder.
- c. Nel campo Nome cartella, fornire una descrizione significativa per report utenti, come "Report Nome Organizzazione".
- d. Fare click su OK per visualizzare la cartella creata sotto Cartelle pubbliche.

Questo crea la struttura minima da utilizzare e memorizza i report della propria organizzazione. Si può aggiungere un numero arbitrario di sottocartelle e di oggetti a questa struttura.

Cambiamenti dello schema all'infrastruttura

Dopo aver stabilito l'ambiente di sviluppo CA BI e aver pubblicato i cambiamenti dello schema in CA Service Desk Manager utilizzando il processo documentato per la personalizzazione dei dati dello schema, le modifiche dello schema sono pronte per essere promosse attraverso l'infrastruttura CA BI. È possibile fare in modo che il nuovo schema sia disponibile per la creazione e la modifica di report.

Aggiunta dei cambiamenti dello schema all'universo derivato

La promozione dei cambiamenti dello schema nell'infrastruttura CA BI è tanto diretta quando l'aggiunta di un nuovo oggetto schema all'universo derivato.

Nota: prima di iniziare, verificare di aver già completato i passaggi corrispondenti, e che gli oggetti del nuovo schema siano stati aggiunti allo schema flessibile CA Service Desk Manager.

Per aggiungere cambiamenti dello schema all'universo derivato

1. Aprire BusinessObjects Designer e importare l'universo derivato a un file system locale come segue:
 - a. Selezionare File, Import dal menu Designer.

Viene visualizzata la finestra di dialogo Importazione universo riuscita.
 - b. Fare clic su OK.

2. Aggiornare la struttura dell'universo derivato come segue:

- Selezionare View, Refresh Structure dal menu Designer.

Vengono visualizzate le seguenti domande:

- "Aggiornare le colonne non aggiornate nelle tabelle selezionate?"
Fare clic su OK.

Nota: se compare il messaggio "Nessun aggiornamento necessario", significa che il livello degli oggetti CA Service Desk Manager non è stato aggiornato correttamente con il nuovo schema. Esaminare i passaggi per la pubblicazione dei cambiamenti dello schema in CA Service Desk Manager.

- "Aggiorna struttura: struttura modificata correttamente". Fare clic su OK.

Compaiono nuove colonne nella struttura dell'universo nel lato destro della finestra, rendendo disponibili nuovi oggetti per l'utilizzo nell'universo derivato.

Gli oggetti sono disponibili per gli strumenti CA BI dopo essere stati spostati dal pannello destro al pannello sinistro. Quando si aggiungono oggetti al pannello sinistro, assicurarsi di seguire gli standard di [modifiche comuni allo schema](#) (a pagina 398).

3. Trascinare i nuovi oggetti nella posizione desiderata nel pannello a sinistra.

4. Fare clic su Salva.

5. Selezionare File, Export dal menu Designer.

Viene visualizzata la finestra di dialogo Universe Successfully Exported.

6. Fare clic su OK.

I cambiamenti aggiunti allo schema dell'universo derivato sono esportati nei CMS locali.

7. Dal menu Designer, selezionare Tools, Check Integrity.

- a. Nella finestra di dialogo che compare, selezionare la casella di controllo Parse Objects. (Non modificare le altre impostazioni.)

- b. Fare clic su OK. Inizia la verifica dell'integrità.

Nota: non devono verificarsi errori di parsing. Se si trovano errori, modificare gli oggetti nel pannello a sinistra in modo che non producano errori di parsing.

8. Fare clic su OK per chiudere la finestra di dialogo.

9. Esportare l'universo derivato nel CMS nel modo seguente:
 - a. Selezionare File, Export dal menu Designer.
 - b. Dall'elenco a discesa del campo Domain, selezionare <Browse>, quindi individuare e selezionare gli universi dei clienti CA.
 - c. Fare click su OK per esportare l'universo al CMS locale
 Viene visualizzata la finestra di dialogo Universe Successfully Exported.
10. Salvare i cambiamenti ed esportare l'universo CA Service Desk Manager.

I cambiamenti sono ora disponibili nell'ambiente di reporting CA BI, compresi i report Web Intelligence e Crystal Reports.

Modifiche dello schema comuni

Si possono implementare modifiche allo schema nell'universo. Per acquisire familiarità con il procedimento, la seguente tabella elenca le modifiche allo schema comuni che si possono trovare.

Quando un tipo di campo è definito in Web Screen Painter come...	Seguire queste regole quando si utilizza il campo nell'universo: Fare click con il tasto destro sull'attributo e selezionare...
INTEGER	Proprietà oggetto, Scheda definizione, Tipo = Numero
STRING	Proprietà oggetto, Scheda definizione, Tipo = Carattere
DATE	Proprietà oggetto, Scheda definizione, Tipo = Data Formato oggetto, scheda Numero: selezionare la categoria "Data/ora"; selezionare il formato mm/gg/aaaa (mese, giorno, anno) hh:mm (ore, minuti)
DURATION	Proprietà oggetto, Scheda definizione, Tipo = Numero; Proprietà oggetto, Scheda definizione, Seleziona = PdmSeconds(object.attr)
SREL	Creare un alias attributo di CA Service Desk Manager.
BREL	Non applicabile
QREL	Non applicabile
DERIVED	Utilizzare un tipo di dati e un formato di oggetto appropriati per il valore memorizzato nel campo derivato, se necessario. Il campo Derivato può produrre qualsiasi risultato, di conseguenza non esiste uno standard specifico da seguire.
Caso speciale: Locale	Il campo Locale è mostrato nel pannello a destra

Quando un tipo di campo è definito in Web Screen Painter come...	Seguire queste regole quando si utilizza il campo nell'universo: Fare click con il tasto destro sull'attributo e selezionare...
Non si tratta di un tipo di dati definito all'interno di Web Screen Painter, anzi, di un tipo di dati utilizzato talvolta dall'universo per indicare un tipo di dati non supportato.	dell'universo con tipo "L". Questi campi possono essere trascinati, ma non rilasciati in una classe nel pannello universo a destra. Spesso, i tipi di dati di campi come binario, non sono supportati dall'universo. Tuttavia, possono essere aggiunti al pannello a sinistra dell'universo creando un oggetto e collocando il PdmString (object.attribute) nella finestra "SELECT" della finestra di dialogo Edit Properties.

Strutture di cartella e report

Sono inclusi nell'installazione di CA BI alcuni oggetti di report Crystal Report XI e WebI. I report sono contenuti nella seguente cartella di CA Service Desk Manager: CA Reports\CA Service Desk Manager.

Importante Non modificare l'universo CA Service Desk Manager e gli oggetti di report contenuti nella struttura di cartelle di CA Service Desk Manager.

Tenere presenti le seguenti informazioni riguardo i report e le strutture di cartelle:

- I passaggi per creare una struttura illustrano come aggiungere una cartella nella sezione pubblica InfoView, che è specifica dell'utente finale. All'interno di questa cartella, un utente può creare sottocartelle e oggetti di report aggiuntivi.
- In un'implementazione in cui ciascun utente è autorizzato ad accedere a CA BI mediante il loro ID di accesso CA Service Desk Manager unico, gli utenti possono salvare i report per uso personale all'interno della sezione My Folders. BusinessObjects mantiene la protezione di questa cartella mostrando questi oggetti solo all'utente che ha effettuato l'accesso.
- In un'implementazione dove tutti gli utenti hanno un ID utente di reporting univoco per l'accesso a CA BI, la sezione My Folders è disponibile a tutti gli utenti.

Creazione di un report di Web Intelligence

Per creare un report Web Intelligence all'interno di CA Business Intelligence

1. Dalla scheda Report CA Service Desk Manager, fare clic sul pulsante InfoView.

Viene visualizzata la pagina iniziale InfoView.

2. Fare clic su New, Web Intelligence Document nella barra dei menu.
3. Selezionare l'universo derivato creato al momento di definire la propria struttura di sviluppo.

Compare lo strumento di creazione di report di Web Intelligence.

Nota: salvare il proprio documento a intervalli regolari. Se la sessione di connessione va in timeout, le modifiche al report andranno perse. Per informazioni su come aumentare il valore di timeout della sessione di connessione Web Intelligence, vedere la *Guida all'amministrazione*.

4. Dalla barra degli strumenti di Web Intelligence, selezionare Save, Save as.
Viene visualizzata la finestra Salva documento.
5. Nella sezione General, specificare un nome significativo per questo report nel campo Title.
6. Nella sezione Location, selezionare la cartella appropriata.
7. (Facoltativo) modificare le proprietà ove richiesto.
8. Fare clic su OK per salvare il report.

Il report compare nella cartella specificata ed è disponibile a tutti gli utenti di report.

Modifica di un report di Web Intelligence

Per modificare un report CA Business Intelligence distribuito nella struttura di cartelle CA Reports\CA Service Desk

1. Dalla scheda Report CA Service Desk Manager, fare clic sul pulsante InfoView.

Viene visualizzata la pagina iniziale InfoView.

2. Nel pannello a sinistra, navigare nella struttura di cartelle di CA Reports, e aprire il report Web Intelligence desiderato.
3. Fare click sul nome del the report in modo che venga avviato e visualizzi un risultato.

4. Dalla barra degli strumenti di Web Intelligence, selezionare Document, Save as.

Viene visualizzata la finestra Salva documento.

5. Nella sezione Location, selezionare la cartella appropriata.
6. Fare click su OK per salvare il report nella nuova ubicazione.
7. Selezionare Document, Edit.
8. Fare clic su Edit Query (il nome dell'universo CA Service Desk Manager viene visualizzato nella scheda Data).
9. Fare clic sulla scheda Properties. Se necessario, fare click sulle frecce in giù accanto all'Universo, in modo da visualizzare il testo CA Service Desk Manager con un segno (...).
10. Fare click sul bottone (...) per mostrare la finestra di dialogo Universo.
Compare la finestra Other Available Universes.
11. Selezionare il nome del proprio universo e fare click su OK.
Web Intelligence eseguirà automaticamente il mapping di tutti i campi noti dall'universo CA Service Desk Manager al proprio universo e visualizzerà la finestra di dialogo Change Source. Compaiono caselle di controllo in verde accanto a ciascun campo mappato. Se tutti i campi sono associati correttamente, fare clic su OK per confermare il cambiamento. Se un campo è visualizzato con una "X" rossa, fare click sul bottone (...) accanto al nome del campo e selezionare il campo appropriato.
12. Dalla barra degli strumenti di Web Intelligence, fare click su Edit Report, e selezionare la scheda Properties.
13. Espandere il nodo General.
14. Fare click sul bottone (...) accanto al valore Document Properties.
Viene visualizzata la finestra di dialogo Proprietà documento.
15. Nella sezione Opzioni documento, selezionare la casella di controllo Aggiorna all'apertura.
16. Fare clic su Save, quindi chiudere Web Intelligence.
Il report è associato al rispettivo universo e può essere modificato ove richiesto.

Creazione di un Crystal Report

Per creare un Crystal Report

1. Aprire Crystal Reports XI.
2. Selezionare File, New, Blank Report.
Viene visualizzata la finestra di dialogo Database Expert.

3. Espandere il nodo Create new Connection e fare click su Universes.
Compare la finestra di dialogo di Business Objects Enterprise.
4. Effettuare l'accesso a BusinessObjects Enterprise utilizzando le credenziali da amministratore.
5. Navigare fino alla cartella contenente l'universo derivato.
6. Selezionare l'universo derivato e fare clic su Open.
Compare la finestra di dialogo Business Objects Query Panel.
7. Nella struttura ad albero Universe, trascinare gli attributi appropriati nelle sezioni Select e Filter del riquadro Query.
8. Quando è terminato il processo di creazione della query, viene presentato lo strumento di progettazione di Crystal Reports standard.
9. Creare e avviare il report.
Nota: per informazioni dettagliate sulla creazione e l'avvio di report, consultare la documentazione di Crystal Reports.
10. Salvare il report nel repository di Business Objects Enterprise come segue:
 - a. Selezionare File, Save as.
 - b. Nella finestra di dialogo Save As, selezionare Enterprise.
 - c. Navigare fino alla cartella creata al momento di definire la struttura di sviluppo, e salvare il nuovo report in BusinessObjects Enterprise.

Il nuovo report sarà ora disponibile nell'azienda e potrà essere modificato in base alle esigenze.

Modifica di un Crystal Report

Per modificare i report di Crystal Reports XI

1. Aprire Crystal Reports XI.
2. Selezionare File, New, Blank Report.
Viene visualizzata la finestra di dialogo Database Expert.
3. Fare click per espandere Create new Connection.
Fare click su Universes.
Compare la finestra di dialogo di Business Objects Enterprise.
4. Effettuare l'accesso in Business Objects Enterprise come amministratore.

5. Fare click per navigare nella cartella che ospita l'universo derivato e fare click per selezionare l'universo derivato.
Fare clic su Open.
Compare la finestra di dialogo Business Objects Query Panel.
6. Accedere alla struttura ad albero Universe per trovare e trascinare gli attributi nelle parti Select e Filter del riquadro Query.
Quando è terminato il processo di creazione della query, a chi stila il report viene presentato lo strumento di progettazione di Crystal Reports standard.
7. Creare e avviare il report in base alle istruzioni di Crystal Reports.
8. Quando si è pronto, salvare il nel repository di Business Objects Enterprise.
 - a. Selezionare File, Save as
Viene visualizzata la finestra Save as.
 - b. Sul lato sinistro della finestra di dialogo Save as, fare clic sull'icona Enterprise.
 - c. Navigare nella struttura di cartelle iniziando con la cartella specifica del cliente creata in precedenza in questo documento e fare click su Save per salvare questo report in Business Objects Enterprise.
9. Il nuovo report sarà disponibile nell'azienda e potrà essere modificato in base alle esigenze.

Spostare i nuovi Crystal Report in CA Business Intelligence

Per spostare i nuovi Crystal Report in CA Business Intelligence

1. Aprire Crystal Reports XI.
2. Selezionare File, Open.
Viene visualizzata la finestra di dialogo Apri.
3. Dal lato sinistro, fare click su Enterprise.
Viene visualizzata la finestra di dialogo per l'accesso a BusinessObjects Enterprise.
4. Effettuare l'accesso a BusinessObjects Enterprise utilizzando le credenziali da amministratore.
Navigare nella struttura di cartelle iniziando da "CA Reports\CA Service Desk" fino a quando non si visualizza il report di destinazione.
5. Selezionare il report di destinazione e dare clic su Open.
Il report appare nei Crystal Reports.

6. Fare clic su File, Save As.

Viene visualizzata la finestra Salva con nome.

7. Specificare la cartella creata al momento di definire la propria struttura di sviluppo.

8. Fare clic su Salva.

9. Dal menù di Crystal Reports, selezionare Database, Database Expert.

Viene visualizzata la finestra di dialogo Database Expert.

10. Dal pannello a sinistra, selezionare Create New Connection, Universe.

11. Selezionare universo derivato.

12. Trascinare tutti gli attributi utilizzati da questo report alla nuova query e fare click su OK.

13. In ogni formula e cella, sostituire gli attributi originali con quelli della nuova query.

14. Dopo la sostituzione di tutti gli attributi, procedere in questo modo:

- a. Selezionare Database, Database Expert dal menù Crystal Reports.

- b. Nella finestra di dialogo Database Expert, selezionare la query originale, e fare click sulle frecce a sinistra al centro dei due pannelli per eliminare la query precedente.

- Se tutti gli attributi sono stati sostituiti correttamente, la query originale sarà rimossa senza problemi e si potrà continuare a modificare il report.
- Se nel report rimangono alcuni attributi originali, viene visualizzato il seguente messaggio: "Il report sta utilizzando campi appartenenti ad una o più tabelle. Continuare?"
- Fare clic su Cancel e ritornare al report.
- Continuare a sostituire tutti gli attributi originali dalla nuova query fino a quando la query originale può essere rimossa senza messaggi di errore.

Il report è pronto per essere personalizzato.

Modalità di spostamento in CA Business Intelligence dei report di accesso esistenti

I report predefiniti di Microsoft Access non vengono più sviluppati o forniti con CA Service Desk Manager. Tuttavia, è possibile spostare i report Access esistenti nell'ambiente di reporting CA Business Intelligence come segue:

1. Aggiungere le modifiche appropriate dello schema di CA Service Desk Manager a CA Business Intelligence.
2. Utilizzare Web Intelligence o Crystal Reports per riscrivere il report.

Passaggio da sviluppo a produzione

A questo punto, è stato aggiunto un universo derivato, sono state create le strutture di cartelle e i report sono stati creati e modificati. Quindi è possibile passare la struttura di sviluppo alla fase di produzione. In questo passaggio, verrà utilizzato BusinessObjects Import Wizard.

Passaggio da sviluppo a produzione

1. Dal menù Start, selezionare Programmi, BusinessObjects XI Release 2, BusinessObjects Enterprise, Import Wizard.
Viene visualizzata la finestra Importazione guidata.
2. Nella schermata Ambiente sorgente, selezionare Business Objects XI R2 e completare le credenziali necessarie per il sistema di sviluppo.
3. Nella schermata Ambiente di destinazione, selezionare *una* delle seguenti opzioni:
 - **Il sistema di produzione.** Questa opzione sposta tutti gli oggetti selezionati immediatamente nel sistema di produzione.
 - **Un file esterno che può essere importato nel sistema di produzione in un secondo momento.** Questa opzione memorizza tutti gli oggetti in un file Business Intelligence Archive Resource (BIAR).
4. Nella schermata Seleziona oggetti da importare, azzerare tutte le impostazioni, quindi selezionare le seguenti caselle di controllo: "Importa cartelle e oggetti" e "Importa Universi".
Nota: ignorare gli avvisi che potrebbero apparire.
5. Selezionare la struttura di cartelle contenente la cartella specifica e deselezionare gli oggetti che non vanno trasferiti.
6. Nella schermata Importa opzioni per universi e connessioni, fare click sull'opzione seguente: "Importa gli universi e le connessioni che i documenti Web Intelligence e Desktop Intelligence utilizzano direttamente."

7. Nella schermata Cartella universo e universi, espandere la cartella corrispondente in cui si trova l'universo.

Nota: ignorare gli avvisi che potrebbero apparire.

8. Fare clic su Fine.

Se le cartelle e i report sono stati spostati direttamente al computer di produzione, è possibile visualizzare i cambiamenti in InfoView. Se gli oggetti sono stati inseriti in un file .biar, utilizzare Import Wizard in un secondo momento, selezionando il file .biar come ambiente sorgente e il server di produzione come ambiente di destinazione.

Personalizzazione di rapporti legacy

CA Service Desk Manager consente di personalizzare rapporti legacy o progettare nuovi rapporti. È possibile:

- Personalizzare riepilogo, dettagli e analisi di rapporti legacy in modo che contengano esattamente le informazioni che interessano, ad esempio aggiungendo campi.
- Produrre un nuovo rapporto con qualsiasi informazione disponibile nel database in un formato utile.
- Passare gli argomenti delle informazioni sulle variabili al rapporto includendo gli argomenti della riga di comando. Gli argomenti possono essere valori o espressioni, ad esempio il valore corrente di un campo o un'espressione della clausola SQL WHERE.
- Generare report dalla riga di comando, da un file script o da un'opzione di menu.

Per creare un rapporto personalizzato

1. Progettare il rapporto:
 - Decidere quali dati includere nel rapporto.
 - Creare un modello di rapporto che contenga query, espressioni e funzioni di tipo-SQL per manipolare i dati e le istruzioni per formattare i dati per la pagina stampata.

2. Generare il rapporto da:

- La riga di comando
- Un'opzione di menu CA Service Desk Manager
- Un file script

Nota: se si dispone di un sistema di database di-terzi, è possibile utilizzarne gli strumenti di generazione dei rapporti per creare rapporti con i dati del database CA Service Desk Manager. CA Service Desk Manager fornisce diverse viste di database che semplificano il processo di creazione di report personalizzati usando sistemi database di terze-parti. Vedere la documentazione relativa al sistema di database usato per informazioni sulla creazione di segnalazioni sui database. Per ulteriori informazioni sulle visualizzazioni di database, consultare la *Guida all'amministrazione*.

Ulteriori informazioni:

[Personalizzazione dei rapporti Crystal Reports](#) (a pagina 432)

Progettazione report personalizzato

Per progettare un rapporto personalizzato, è necessario avere una conoscenza di base dei concetti seguenti:

- Scrittura di query SQL.
- Programmazione, specialmente in C.
- Creazione di programmi o file script speciali da eseguire prima del programma del modello di rapporto. Ad esempio, è possibile creare un programma che richieda all'utente di immettere un argomento, ad esempio le condizioni per una clausola WHERE.

Nota: prima di creare un rapporto personalizzato, verificare che il rapporto non sia stato già fornito. CA Service Desk Manager fornisce un'ampia gamma di report Crystal e Microsoft Access e versioni runtime di questi prodotti che consentono di eseguire i report. Per ulteriori informazioni sui rapporti, consultare la *Guida all'amministrazione*.

Selezione di informazioni per il rapporto

Per selezionare i dati dal database CA Service Desk Manager dei report personalizzati, vedere la *Guida di riferimento tecnico* di *CA Service Desk Manager*. L'appendice elenca le tabelle, i campi, le descrizioni e altre informazioni relative ai database.

Modalità di creazione di un modello di report

Un modello di rapporto è un file che, quando viene eseguito da un apposito programma CA Service Desk Manager, genera un rapporto di tipo particolare. Un modello di rapporto contiene espressioni di variabili, funzioni e istruzioni che definiscono come i dati vengono caricati, calcolati e stampati.

Per creare un modello di rapporto, creare un file contenente i tipi seguenti di istruzioni:

Istruzioni di blocco

Usate per definire le tabelle di database CA Service Desk Manager da cui verranno caricati i dati e le azioni da eseguire sui dati caricati.

Istruzioni di layout

Usate per definire come le variabili di dati e il testo normale vengono visualizzati nell'output del rapporto.

Nota: memorizzare tutti i file .rpt in una nuova directory, \$NX_ROOT/site/mods/rpt (UNIX) o *directory-installazione*\site\mods\rpt (Windows). In questo modo i file vengono conservati quando si esegue l'aggiornamento a una nuova release di CA Service Desk Manager.

Ulteriori informazioni:

[Riferimenti per un modello di rapporto](#) (a pagina 416)

[Esempio: modello di rapporto](#) (a pagina 412)

Istruzioni BLOCK

Le istruzioni BLOCK forniscono la struttura del rapporto. Definiscono i dati da manipolare e controllano l'esecuzione del rapporto. Le istruzioni BLOCK iniziano con un nome che deve essere univoco in tutto il modello di rapporto. Sono composte dalle due sezioni seguenti:

Sezione query dei dati

Contiene le clausole SQL SELECT, WHERE e SORT per definire quali dati verranno caricati dal database.

Sezione programma di output

Definisce le azioni che devono essere eseguite sui dati caricati. Contiene dichiarazioni di variabili, funzioni e altre istruzioni BLOCK, comprese istruzioni nidificate, che possono essere usate per creare report condizionali. Può contenere anche istruzioni di layout che formattano e stampano i dati come testo ASCII.

Di seguito è riportata una versione semplificata della sintassi di un'istruzione BLOCK che mostra la relazione tra le due sezioni:

BLOCK *nomeblocco* ("SELECT clause", "WHERE clause")

 SORT clause {*istruzioni programma di output*}

Nella parte BLOCK, in Riferimenti per un modello di report, vengono descritti la versione completa della sintassi e ogni clausola e parametro.

Istruzioni di layout nei modelli di rapporto

Le istruzioni di layout definiscono come le variabili di dati e il testo normale vengono visualizzati nell'output del rapporto:

- È possibile usare le istruzioni PAGE HEADER e PAGE FOOTER per inserire informazioni nella parte superiore e inferiore di ogni pagina del rapporto.
- Le istruzioni HEADER, HEADER2, FOOTER e PRINT possono essere nidificate all'interno della sezione con le parentesi graffe dell'istruzione BLOCK principale per creare titoli e totali riepilogativi per le varie *sezioni dei dati del reporting* (parti dell'output del report).

Nota: quando si effettua una nidificazione, prestare attenzione a non confondere le parentesi graffe usate nelle istruzioni di layout con le parentesi graffe che racchiudono le istruzioni nidificate all'interno di un'istruzione BLOCK principale.

- È possibile includere testo normale per creare etichette e tracciare linee con dei caratteri per migliorare l'aspetto del rapporto.

Le istruzioni di layout sono le seguenti:

PAGE HEADER

Inserisce informazioni nella parte superiore di ogni pagina del rapporto. Va scritta all'esterno dell'istruzione BLOCK.

PAGE FOOTER

Inserisce informazioni nella parte inferiore di ogni pagina del rapporto. Va scritta all'esterno dell'istruzione BLOCK.

HEADER

Inserisce informazioni nella parte superiore di ogni sezione dei dati del reporting. Va scritta all'interno dell'istruzione BLOCK.

HEADER2

Inserisce il seguito delle informazioni dell'intestazione nella parte superiore di ogni pagina successiva di una sezione dei dati del reporting, se questa sezione occupa più pagine. Va scritta all'interno dell'istruzione BLOCK.

FOOTER

Inserisce informazioni nella parte inferiore di ogni sezione dei dati del reporting. Va scritta all'interno dell'istruzione BLOCK.

PRINT

Inserisce i dati in una sezione dei dati del reporting. Va scritta all'interno dell'istruzione BLOCK.

Nelle istruzioni di layout possono essere usate anche le variabili predefinite seguenti:

- CT (stampa l'ora corrente)
- CD (stampa la data corrente)
- PG (stampa il numero di pagina)

Campi di dati

Specifica qualsiasi variabile in un'istruzione di layout che dà come risultato una parte di dati quando si genera il report. Seguire le indicazioni seguenti per inserire i campi nel modello di rapporto:

- Racchiudere i campi di dati in parentesi quadre ([]).
- Le parentesi quadre del campo definiscono il relativo spazio di stampa in ogni riga di output. Questo spazio è il numero di caratteri delimitati dalle parentesi quadre, parentesi comprese. Se l'output di una variabile è più lungo dello spazio di stampa, viene troncato. Per assicurarsi che il campo abbia uno spazio di stampa sufficiente, è possibile aggiungere spazi finali tra il nome della variabile e la parentesi di chiusura. Ad esempio, questi spazi consentono di inserire i nomi lunghi dei contatti:

[contact]

- Se l'output è più corto di una riga, il campo può essere delimitato da una parentesi angolare di chiusura (>). In questo modo lo spazio di stampa viene esteso al margine destro. Ad esempio, la parentesi angolare di chiusura usata in un'istruzione HEADER consente di stampare la data corrente senza troncarla:

```
[CD      >
```

Nota: quando il campo è più lungo di una riga e la variabile è contrassegnata come MULTILINE, la parentesi angolare di chiusura (>) compie la stessa azione della parentesi quadra di chiusura (]). Se l'istruzione PRINT per una variabile MULTILINE viene delimitata da una parentesi angolare di chiusura (>), i caratteri ricoprono gli spazi per adattarsi al campo definito dalla parentesi quadra di apertura ([) e dalla parentesi angolare di chiusura (>). Se la variabile non è MULTILINE, l'uso della parentesi angolare consente di visualizzare tutti i dati sulla riga corrente indipendentemente dalla lunghezza.

- Un campo in un'istruzione di layout può fare riferimento al nome di una variabile o di una colonna definiti in precedenza.
- Per fare riferimento al nome di una variabile o di una colonna in un'altra istruzione BLOCK, usare la sintassi seguente:

```
nomeblocco::colonna | nome-variabile
```

Testo normale

Il testo normale consente di includere informazioni supplementari nel rapporto. Viene visualizzato nell'output del rapporto esattamente come specificato nel modello. Per includere un testo in un'istruzione di layout, inserirlo in una riga qualsiasi dopo la parentesi graffa di apertura ({) e prima della parentesi graffa di chiusura (}). Non racchiuderlo tra virgolette o parentesi quadre.

In questo esempio le parole "Azienda ACME" e "Pagina: " sono interpretate come testo normale dal programma dei report CA Service Desk Manager:

```
PAGE HEADER {
    Azienda ACME      Pagina: [PG]
}
```

Ulteriori informazioni:

[Istruzioni FOOTER del modello di rapporto](#) (a pagina 426)
[Istruzione PAGE FOOTER del modello di rapporto](#) (a pagina 429)
[Istruzioni HEADER del modello di rapporto](#) (a pagina 427)
[Istruzioni HEADER2 del modello di rapporto](#) (a pagina 428)
[Istruzione PAGE HEADER del modello di rapporto](#) (a pagina 430)
[Istruzioni PRINT del modello di rapporto](#) (a pagina 430)

Espressioni di variabili nel modello di rapporto

Ogni valore che si desidera visualizzare nell'output del rapporto può essere assegnato a una variabile. Le espressioni di variabili consentono di:

- Manipolare i dati CA Service Desk Manager.
- Usare le funzioni per eseguire calcoli sui valori caricati.

L'esempio seguente mostra come creare una variabile chiamata *desc* per fare riferimento al contenuto del campo *chg_desc* nella finestra Ordine di cambiamento. Il flag MULTILINE consente di stampare interamente la variabile su più righe:

```
desc = description MULTILINE;
```

L'esempio seguente mostra come viene stampata la descrizione. La lunghezza dell'output sarà quella definita nelle parentesi. Se si desidera visualizzare una descrizione più lunga, aumentare il numero di spazi nelle parentesi.

```
PRINT { [desc ] }
```

Esempio: modello di rapporto

Il modello di rapporto seguente, Rapporto contatto interessato, indica come creare un modello di rapporto e genera un rapporto che elenca gli ordini di cambiamento aperti con lo stesso contatto:

```
PAGE HEADER {  
    As Of: [CD>  
    [CT>  
}  
PAGE FOOTER {  
    Pagina: [PG>  
}  
BLOCK chg ("SELECT \  
    chg_ref_num, description, priority, \  
    status, category, assignee \  
    FROM Change_Request",  
    "WHERE #Change_Request.status = 'OP' \  
    AND #Change_Request.requestor = #ca_contact.id \  
    AND #ca_contact.last_name = ? \  
    AND #ca_contact.first_name = ? \  
    AND #ca_contact.middle_name = ? ", $1, $2, $3)  
{  
    BLOCK st ("SELECT sym FROM Change_Status",  
    "WHERE code = ? ", chg::status) {}  
    BLOCK (strlen(category)) cat ("SELECT sym FROM Change_Category",  
    "WHERE code = ? ", chg::category) {}
```

```

HEADER {
    OPEN CHANGE ORDERS WITH SAME REQUESTOR/FROM CONTACT
    CHANGE ORDER Summary    Pri Status Category    Assignee
}
HEADER2 {
    CHANGE ORDER Summary    Pri Status Category    Assignee
    -----
}

    num = chg_ref_num;
    desc = description MULTILINE;
    pr = deref (priority);
    stat = st::sym;
    catgry = cat::sym;
    asgn = deref (assignee);
PRINT {
[num ] [desc ] [pr ] [stat ] [catgry ] [asgn ]
}
}

```

Page Header

Specifica che cosa stampare nella parte superiore di ciascuna pagina del report. CD e CT sono variabili predefinite che forniscono la data e l'ora correnti e vengono visualizzate nell'intestazione sulla parte superiore di ogni pagina. Ognuno di questi campi termina con una parentesi angolare per permettere al campo di espandersi verso il margine destro. Poiché la stringa "As Of:" è all'esterno di un campo e sulla riga successiva alla parentesi graffa di apertura, verrà visualizzata come testo normale nell'output del rapporto.

```

PAGE HEADER {
    As Of: [CD>
    [CT>
}

```

Page Footer

Include il numero di pagina con "Pagina: " come testo.

```

PAGE FOOTER {
    Pagina: [PG>
}

```

Nota: poiché le istruzioni PAGE HEADER e PAGE FOOTER generano intestazioni e piè di pagina globali, non vengono incluse nelle istruzioni BLOCK.

Sezione di segnalazione

Crea una sezione di reporting per l'istruzione BLOCK principale, insieme alle sue istruzioni nidificate. Questa sezione costituisce solo una parte del rapporto ma in questo caso il rapporto è composto da una sola sezione. Il nome univoco di questo blocco è chg.

La clausola SELECT seleziona le colonne da includere nei dati del rapporto ricavate da tre tabelle ma solo quando sono soddisfatte le condizioni specificate dalla clausola WHERE.

Le ultime tre espressioni AND nella clausola WHERE contengono punti interrogativi che agiscono da segnaposto di argomenti che assumono i valori degli argomenti \$1, \$2 e \$3. Pertanto, \$1 rappresenta ca_contact.last_name, \$2 rappresenta ca_contact.first_name e \$3 rappresenta ca_contact.middle_name. Gli argomenti \$1, \$2 e \$3 ricevono i valori degli argomenti della riga di comando.

```
BLOCK chg ("SELECT \
...",
"WHERE \
...\
AND #ca_contact.last_name = ? \
AND #ca_contact.first_name = ? \
AND #ca_contact.middle_name = ? ", $1, $2, $3)
```

Intestazioni della sezione di segnalazione

Specifica che la parentesi graffa di apertura inizia la parte di output del programma dell'istruzione BLOCK: le sue istruzioni indicano che cosa fare con i dati caricati dalle clausole SELECT e WHERE. Questo esempio mostra le istruzioni HEADER e HEADER2 nidificate che verranno applicate solo a questa sezione di segnalazione. HEADER2 viene stampata solo se l'output del rapporto si estende su più pagine.

```
{
...
  HEADER {
    OPEN CHANGE ORDERS WITH SAME REQUESTOR/FROM CONTACT
    CHANGE ORDER Summary      Pri  Status Category Assignee
  }
  HEADER2 {
    CHANGE ORDER Summary      Pri  Status Category Assignee
    -----
  }
}
```

Assegnazioni delle variabili

Determina espressioni di variabili che agiscono sui dati specificati dalle clausole SELECT. Le variabili vengono assegnate ai valori delle colonne e ai risultati delle espressioni. Queste variabili corrispondono ai campi dell'istruzione PRINT descritti di seguito.

Il flag MULTILINE sulla variabile *desc* consente di stamparla o visualizzarla su più righe per evitare che venga troncata. La funzione *deref* viene usata per restituire l'espressione della stringa contenuta nelle colonne a cui si fa riferimento.

```
num = chg_ref_num;
desc = description MULTILINE;
pr = deref (priority);
stat = st::sym;
catgry = cat::sym;
asgn = deref (assignee);
```

Stampa

Contiene i campi da stampare. Questa istruzione potrebbe includere anche righe di testo normale per migliorare l'aspetto del rapporto. La parentesi graffa di chiusura chiude la sezione del programma di output dell'istruzione BLOCK iniziata con la parentesi graffa di apertura.

```
PRINT {
[num ][desc ][pr][stat][catgry][asgn ]
}
}
```

Ulteriori informazioni:

[Comando report](#) (a pagina 416)

Modalità di generazione dei report

Dopo aver creato il modello di rapporto, è possibile generare il rapporto eseguendo il relativo programma CA Service Desk Manager. Il programma può essere eseguito da:

- La riga di comando
- Un'opzione di menu CA Service Desk Manager
- Un file script

Nota: se si lavora su un server UNIX, è possibile includere nel comando il parametro di reindirizzamento dell'output del rapporto (*rptuiDsp*) per visualizzare una finestra di dialogo con le opzioni per inviare il rapporto a video, a un file o alla stampante.

Ulteriori informazioni:

[Modalità di visualizzazione di una finestra di dialogo \(solo UNIX\)](#) (a pagina 416)

Comando report

Per generare un rapporto dalla riga di comando, in UNIX, è necessario usare il comando report CA Service Desk Manager:

```
pdm_task report [-h][-e][-f][-F stringaff][-p lunghezzapagina] nomefile [argomenti-riga-comando]
```

Nota: il comando report è preceduto dal comando pdm_task che imposta le variabili di ambiente necessarie. Se il rapporto prevede l'accettazione degli argomenti della riga di comando, è necessario immettere 1 per ogni argomento nel modello di rapporto.

In Windows, usare il comando rpt_srv:

```
rpt_srv titolo-report
```

L'esempio seguente include i tre argomenti della riga di comando (Smith, Jane e L) necessari per il Rapporto contatto interessato, descritto nell'esempio di un modello di rapporto, nella parte precedente di questo capitolo:

```
pdm_task report /reports/myrpt.rpt Smith Jane L
```

Se un argomento è vuoto, è necessario usare una stringa nulla. Ad esempio, se Jane Smith non ha l'iniziale del secondo nome, la sintassi è:

```
pdm_task report /reports/myrpt.rpt Smith Jane ""  
rpt_srv /reports/myrpt.rpt Smith Jane L
```

Modalità di visualizzazione di una finestra di dialogo (solo UNIX)

Per visualizzare una finestra di dialogo, è possibile includere il parametro di reindirizzamento dell'output del rapporto (rptuiDsp) nel comando report. La finestra di dialogo visualizza le opzioni per stampare il rapporto su un file, visualizzarlo in una finestra Xterm o inviarlo alla stampante.

Esempio:

```
pdm_task rptuiDsp report /reports/myrpt.rpt Smith Jane L
```

In questo esempio, il titolo "Rapporto inventario" viene aggiunto alla finestra di dialogo:

```
pdm_task rptuiDsp report /reports/myrpt.rpt Smith Jane L "title:Rapporto inventario"
```

Riferimenti per un modello di rapporto

È possibile utilizzare espressioni variabili, funzioni, e istruzioni in un modello di report.

Espressioni di variabili del modello di rapporto

Le espressioni di variabili definiscono i dati da stampare o visualizzare. Vanno scritte in un'istruzione di layout o BLOCK.

Sintassi

Per sintassi si intendono le regole che governano la scrittura delle istruzioni in un linguaggio di programmazione. Di seguito è riportata la struttura di una stringa:

nome-variabile = espressione [flag]

Flag

I flag formattano il risultato di un'espressione di variabili. Usare questi flag per formattare i campi di testo:

MULTILINE

Visualizza i dati su più righe per evitare che vengano troncati.

RIGHT

Giustifica a destra.

Usare questi flag per formattare i campi numerici:

BLANKZERO

Agisce come un campo con valore-nullo che non stampa uno zero.

BOOL

Converte lo zero in "no" o un valore diverso da-zero in "sì".

REAL

Visualizza i numeri a virgola mobile (il valore predefinito è l'intero).

ZEROFILL

Mostra gli zeri iniziali o finali.

Usare questi flag per formattare i campi della data e dell'ora:

DATE

Mostra solo la data.

DAYS

Visualizza la durata in giorni.

HOURS

Visualizza la durata in ore.

MINUTES

Visualizza la durata in minuti.

SECONDS

Visualizza la durata in secondi.

TIME

Mostra solo l'ora.

Esempio

desc = description MULTILINE

Commenti

I nomi delle variabili devono essere univoci in un'istruzione BLOCK e devono essere diversi da quelli delle colonne nella clausola SELECT del blocco. Lo stesso nome di variabile può essere usato in diverse istruzioni BLOCK ma non può essere ripetuto all'interno di una stessa istruzione BLOCK.

Attenersi a queste regole della sintassi quando si includono espressioni nel modello di rapporto:

- Usare qualsiasi espressione C valida.
- Non racchiudere nomi di variabili o colonne tra virgolette.
- Racchiudere le costanti di stringa tra apici o virgolette.
- È possibile fare riferimento a un blocco nidificato ma solo se contiene esattamente una riga.
- Per includere il nome di una colonna uguale a una parola chiave, inserire una barra rovesciata (\) davanti al nome. Ad esempio, ALIAS è una parola chiave e \alias è il nome di una colonna.
- Usare il simbolo del dollaro (\$) per fare riferimento alle variabili di ambiente, ad esempio \$name, e per fare riferimento agli argomenti della riga di comando, ad esempio \$n, dove *n* rappresenta la posizione dell'argomento nella riga di comando.

- Per specificare il numero argomenti della riga di comando, usare `$#`. Ad esempio, l'espressione seguente significa che se il numero di argomenti della riga di comando è maggiore di 1, usare l'argomento aggiuntivo come un argomento altrimenti impostare il valore dell'argomento su una stringa vuota. Il modello di rapporto stesso è considerato un argomento della riga di comando. Pertanto il numero di argomenti è almeno 1.

```
$# > 1 ? $1 : "
```

- Usare `##` per concatenare due stringhe, ad esempio:

```
title = "Questa è la " ## "prima riga. "
```

```
long_name = fn
```

```
  first_name ## last_name
```

- Sono supportati i cast seguenti:

- (number)
- (string)
- (date_time)
- (duration)

- Per fare riferimento al nome di una variabile o di una colonna in un altro blocco, mettere davanti a questo nome il nome del blocco e due segni di due punti. Ad esempio:

```
nomeblocco::colonna | nome-variabile
```

Funzioni del modello di rapporto

Nel modello di rapporto possono essere usate le funzioni seguenti:

is_null (*espressione*)

Questa funzione restituisce il valore true se l'espressione è nulla.

```
false = 0
```

```
true = is_null (false)
```

sqrt (*espressione*)

Questa funzione calcola la radice quadrata dell'espressione.

```
nine = 9
```

```
three = sqrt (nine)
```

pow (*espressione1*, *espressione2*)

Questa funzione eleva l'*espressione1* alla potenza indicata dall'*espressione2*.

```
two = 2
```

```
three = 3
```

```
eight = pow (two,three)
```

log (*espressione*, *espressione*)

Questa funzione calcola il logaritmo naturale dell'espressione.

```
ten = 10
```

```
result = log (ten)
```

catname (*espressione*, *espressione*, *espressione*)

Questa funzione concatena tre stringhe che rappresentano il nome di un contatto in una stringa usando le virgole, secondo le regole del file del formato dei campi.

```
last = "Murphy"
```

```
first = "Fred"
```

```
middle = "P"
```

```
contact_name=catname (last, first, middle)
```

strlen (*stringa*)

Questa funzione restituisce la lunghezza della stringa.

```
buffer = "Stringa di trenta caratteri"
```

```
thirty = strlen(buffer)
```

strindex (*stringa*, *pattern* [, *avvio_indice*])

Questa funzione restituisce l'indice della prima ricorrenza di *pattern* o di quella successiva dopo *start_index*, nella stringa. Restituisce -1 se non vi sono ricorrenze.

```
buffer = "Stringa di trenta caratteri"
```

```
zero = strindex(buffer, "[A-Z]")
```

```
due = strindex(buffer, "[a-z]")
```

substr (*stringa*, *pattern* [, *lunghezza*])

Questa funzione restituisce la parte della stringa che segue la prima ricorrenza di *pattern*. Se la *lunghezza* è definita, limita la lunghezza della stringa di output. Restituisce una stringa di lunghezza zero se non vi sono ricorrenze.

```
buffer = "Stringa di trenta caratteri"
```

```
last_word = substr(buffer, "[a-z]*$")
```

```
first_capital_letter = substr(buffer, "[A-Z]",
```

```
1)
```

substr (*stringa*, *indice* [, *lunghezza*])

Questa funzione restituisce la porzione della stringa dopo l'indice. La sua *lunghezza* è definita e limita la lunghezza della stringa di output. Restituisce una stringa di lunghezza zero se non vi sono ricorrenze.

```
buffer = "Riepilogo: la scheda di rete mostra un
```

```
codice di ..
```

```
summary = substr(buffer, 9)
```

```
30_char_summary = strindex(buffer, 9, 30)
```

Le funzioni rimanenti (pseudofunzioni) vengono eseguite su un blocco di dati anziché sulle espressioni di variabili. Di solito queste funzioni vengono inserite in un'istruzione BLOCK per ottenere informazioni sui dati di un'istruzione BLOCK nidificata.

count (*nome-blocco*)

Restituisce il numero di righe nel blocco specificato nell'istruzione BLOCK. Nome-blocco deve essere una stringa semplice.

```
BLOCK sample ("SELECT id FROM Contact") {  
  
  entries = count (sample)  
  
}
```

sum (*nome-blocco, espressione*)

Esegue l'espressione per ogni riga del blocco specificato e ne somma i risultati.

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request") {  
  
  difference = sum (sample, est_cost-actual_cost)  
  
}
```

average (*nome-blocco, espressione*)

Esegue l'espressione per ogni riga del blocco specificato e restituisce la media dei risultati.

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request"){  
  
  avg_difference = average (sample, est_cost-actual_cost)  
  
}
```

prev (*espressione*)

Restituisce il valore precedente dell'espressione. Questa funzione dovrebbe essere usata con attenzione in modo che il relativo valore non sovrasciva inavvertitamente l'ultimo valore.

downtime (*sla_pianificazione, espressione1, espressione2 [, ritardo-blocco, espressione, espressione]*)

Richiama il calcolo dei tempi inattivi dello SLA. Il primo argomento deve essere una stringa che identifica un turno. Gli altri argomenti sono orari di inizio e fine:

espressione1 è la data/ora di inizio dell'evento

espressione2 è la data/ora di fine dell'evento

In questo esempio, l'istruzione BLOCK wrkshft carica la pianificazione dei turni, l'istruzione BLOCK evt_dly carica i ritardi e la funzione downtime usa questi record per calcolare i tempi inattivi.

```
BLOCK attevt ("SELECT start_time, fire_time, event_tmpl, obj_id FROM
Attached_Events")
```

```
{
BLOCK evt ("SELECT persid, sym, work_shift FROM Events ", "WHERE persid = ?", attevt::event_tmpl) {}
BLOCK wrkshft ("SELECT sched FROM Bop_Workshift", "WHERE persid = ?", evt::work_shift) {}

BLOCK evt_dly ("SELECT start_time, stop_time FROM Event_Delay", "WHERE obj_id = ?", attevt::obj_id)
{}
total_downtime = downtime(wrkshft::sched,
attevt::start_time, attevt::fire_time,
evt_dly,
evt_dly::start_time, evt_dly::stop_time);
}
```

deref (nome-colonna)

Restituisce la rappresentazione come stringa del puntatore eseguendo una ricerca automatica nella tabella appropriata.

```
BLOCK chg ("SELECT organization FROM Change_Request") {
org = deref (organization)
}
```

Poiché questa pseudofunzione implica le ricerche, è valida solo se è l'unico elemento nell'espressione. Di seguito viene fornito un esempio di pseudofunzione valida:

```
model = deref (nr_model)
```

Di seguito viene fornito un esempio di pseudofunzione non valida:

```
model = "model" ## deref (nr_model)
```

Nota: non è consentito inoltrare i riferimenti alle variabili o ai blocchi.

Istruzioni BLOCK del modello di rapporto

Le istruzioni BLOCK definiscono le tabelle di database dalle quali verranno caricati i dati e possono includere le azioni da eseguire sui dati caricati.

Sintassi

Per sintassi si intendono le regole che governano la scrittura delle istruzioni in un linguaggio di programmazione. Di seguito è riportata la struttura di una stringa con BLOCK:

```
BLOCK nomeblocco (  
    "SELECT [ALIAS.] nome_campo[, nome_campo ...]  
    FROM nome_tabella[, nome_tabella ...]"  
    [,"WHERE clausola_where"][, argomenti.])  
    [SORT "clausola_sort"]  
{  
    istruzioni del programma di output  
}
```

Parametri

nomeblocco

Identifica il blocco. Ogni *nomeblocco* deve essere univoco.

Clausola SELECT

Segue il *nomeblocco* ed è delimitata dalle virgolette. Elenca le colonne da caricare, seguite dalla parola chiave FROM, seguita dalle tabelle da cui devono essere caricate le colonne. È una clausola obbligatoria. Ecco un esempio in cui sono specificate tre tabelle:

```
"SELECT open_date, chg_ref_num \  
last_name, first_name \  
FROM Change_Request, \  
ca_contact"
```

Non è possibile includere un alias SQL, ad esempio:

```
"SELECT open_date As OpenDate"
```

WHERE, clausola

(Opzionale) Segue la clausola SELECT e qualifica ulteriormente le informazioni selezionate. Può essere una costante di stringa o un'espressione da valutare rispetto a una stringa. Se la clausola WHERE è costituita da una stringa vuota, vengono restituiti tutti i record. Le clausole WHERE possono contenere argomenti di sostituzione (che fanno riferimento a variabili o argomenti della riga di comando) per mezzo del punto interrogativo (?). La clausola WHERE riportata di seguito potrebbe seguire la clausola SELECT indicata in precedenza:

```
"WHERE #Change_Request.open_date >= ? \  
AND #Change_Request.active_flag = 1 \  
AND #ca_contact.last_name = ? ", $1
```


Nota: la clausola WHERE deve essere separata dalla clausola SELECT, perché la clausola WHERE può essere un'espressione di valutazione rispetto a una stringa mentre la clausola SELECT è esclusivamente una costante di stringa. Ciò offre maggiori flessibilità e capacità di manipolazione dei dati nella generazione del proprio rapporto.

Clausola SORT

(Opzionale) Segue le clausole SELECT e WHERE e ordina le righe caricate dei dati. La clausola SORT ha il formato della clausola SQL ORDER BY. Ecco un esempio:

```
SORT "open_date"
```

Istruzioni del programma di output

Controlla l'esecuzione del rapporto. Prima della query dei dati, l'istruzione HEADER, se inclusa, stampa il test a caldo del blocco. Quindi viene eseguita la query dei dati. Se vengono restituiti dati, ogni istruzione viene eseguita nell'ordine scritto, con un'eccezione. Le funzioni di blocco, come la somma e la media, si comportano come se stessero alla fine del programma di output. Infatti, i loro valori non sono stabili finché non inizia l'esecuzione del record di dati successivo.

Importante Il programma output dipende dal successo della query di dati. Se dalla query non viene restituito nessun dato, tranne quelli dell'istruzione HEADER, il programma di output non verrà eseguito.

Esempio

Questa istruzione BLOCK presuppone che venga passato un argomento contenente un numero intero uguale alla priorità dell'ordine di cambiamento. La clausola WHERE prima controlla il numero di argomenti passati (\$#). Se è presente un argomento, viene usato per valutare l'espressione per produrre la clausola WHERE; altrimenti viene usata una clausola WHERE nulla (" ").

```
BLOCK chg ("SELECT priority FROM Change_Request",
$# > 1 ? "WHERE priority =" ## $1 : " ") {}
```

Esempio

```
FOOTER {
  Informazioni di riepilogo:
    Totale errori: [Fail_count >
    Totale inattività: [Downtime >
}
```

Commenti

Le istruzioni HEADER, HEADER2, FOOTER, PRINT e le espressioni di variabili possono essere inserite tra parentesi graffe. Ogni istruzione verrà eseguita per ogni riga selezionata.

Nota: le istruzioni PAGE HEADER e PAGE FOOTER non possono essere inserite in un'istruzione BLOCK.

Istruzioni FOOTER del modello di rapporto

Questa istruzione di layout inserisce le informazioni nella parte inferiore di una sezione dei dati del reporting.

Sintassi

Per sintassi si intendono le regole che governano la scrittura delle istruzioni in un linguaggio di programmazione. Di seguito è riportata la struttura di una stringa con FOOTER:

FOOTER {parametri}

Parametri

I parametri sono i seguenti:

CD

Una variabile predefinita usata per visualizzare la data corrente.

CT

Una variabile predefinita usata per visualizzare l'ora corrente.

PG

Una variabile predefinita usata per visualizzare il numero di pagina corrente.

nome-colonna | nome-variabile

Questo campo può essere una variabile ricavata da un'espressione di variabili precedente o un riferimento a una colonna nella clausola SQL di un'istruzione BLOCK.

testo normale

Qualsiasi testo che non sia il nome di una variabile predefinita o di una colonna viene interpretato come testo normale. Il testo normale incluso nell'istruzione FOOTER viene visualizzato in orizzontale esattamente dove è stato digitato.

Commenti

Le istruzioni FOOTER vengono stampate nella parte inferiore di una sezione dei dati del reporting. Di solito vengono usate per presentare informazioni o statistiche riepilogative. È possibile includere un'istruzione FOOTER in un'istruzione BLOCK.

Il contenuto di un campo occupa esattamente lo spazio racchiuso tra le parentesi quadre. Qualsiasi carattere in più viene troncato. Tuttavia, è possibile chiudere un campo con una parentesi angolare di chiusura (>) per permettere di espandere il campo in tutta la sua lunghezza verso il margine destro.

Per fare riferimento al nome di una variabile o di una colonna in un'altra istruzione BLOCK, usare la sintassi seguente:

nomeblocco::colonna | nome-variabile

Istruzioni HEADER del modello di rapporto

Questa istruzione di layout inserisce le informazioni nella parte superiore di una sezione dei dati del reporting.

Sintassi

Per sintassi si intendono le regole che governano la scrittura delle istruzioni in un linguaggio di programmazione. Di seguito è riportata la struttura di una stringa con HEADER:

HEADER {*parametri*}

Parametri

Per un elenco e una spiegazione dei parametri validi per questa istruzione, vedere [Istruzioni PAGE HEADER del modello di rapporto](#) (a pagina 430).

Esempio

```
HEADER {  
    Rapporto riepilogo contatto  
    Nome contatto Alias contatto Organizzazione  
}
```

Commenti

Le istruzioni HEADER vengono stampate all'inizio di una sezione dei dati del reporting e possono essere incluse in un'istruzione BLOCK. Di solito le istruzioni HEADER vengono usate per presentare le intestazioni di sezioni e/o colonne.

Il contenuto di un campo occupa esattamente lo spazio racchiuso tra le parentesi quadre. Qualsiasi carattere in più viene troncato. Tuttavia, è possibile chiudere un campo con una parentesi angolare di chiusura (>) per permettere di espandere il campo in tutta la sua lunghezza verso il margine destro.

Nota: se l'istruzione PRINT per una variabile MULTILINE viene delimitata da una parentesi angolare di chiusura (>), i caratteri ricoprono gli spazi per adattarsi al campo definito dalla parentesi quadra di apertura ([) e dalla parentesi angolare di chiusura (>). Se la variabile non è MULTILINE, l'uso della parentesi angolare consente di visualizzare tutti i dati sulla riga corrente indipendentemente dalla lunghezza.

Per fare riferimento al nome di una variabile o di una colonna in un'altra istruzione BLOCK, usare la sintassi seguente:

nomeblocco::colonna | nome-variabile

Istruzioni HEADER2 del modello di rapporto

Questa istruzione di layout inserisce il seguito delle informazioni dell'intestazione nella parte superiore di ogni pagina successiva di una sezione dei dati del reporting, se questa sezione occupa più pagine.

Sintassi

Per sintassi si intendono le regole che governano la scrittura delle istruzioni in un linguaggio di programmazione. Di seguito è riportata la struttura di una stringa con HEADER2:

HEADER2 {parametri}

Parametri

Per un elenco e una spiegazione dei parametri validi per questa istruzione, vedere [Istruzioni HEADER2 del modello di rapporto](#) (a pagina 428).

Esempio

```
HEADER2 {  
  Rapporto riepilogo contatto (seguito)  
  Nome contatto  Alias contatto  Organizzazione  
}
```

Commenti

Un'istruzione HEADER2 può essere inclusa in un'istruzione BLOCK.

Il contenuto di un campo occupa esattamente lo spazio racchiuso tra le parentesi quadre. Qualsiasi carattere in più viene troncato. Tuttavia, è possibile chiudere un campo con una parentesi angolare di chiusura (>) per permettere di espandere il campo in tutta la sua lunghezza verso il margine destro.

Per fare riferimento al nome di una variabile o di una colonna in un'altra istruzione BLOCK, usare la sintassi seguente:

nomeblocco::colonna | nome-variabile

Istruzione PAGE FOOTER del modello di rapporto

Questa istruzione di layout inserisce le informazioni nella parte inferiore di ogni pagina del rapporto.

Sintassi

PAGE FOOTER {*parametri*}

Parametri

Ad eccezione del fatto che non è possibile usare i nomi di colonne e variabili, i parametri per questa istruzione sono gli stessi per FOOTER. Per un elenco e una spiegazione dei parametri validi per questa istruzione, vedere [Istruzione PAGE FOOTER del modello di rapporto](#) (a pagina 429).

Esempio

```
PAGE FOOTER {  
    Numero di pagina: [PG>  
}
```

Commenti

Il contenuto di un campo occupa esattamente lo spazio racchiuso tra le parentesi quadre. Qualsiasi carattere in più viene troncato. Tuttavia, è possibile chiudere un campo con una parentesi angolare di chiusura (>) per permettere di espandere il campo in tutta la sua lunghezza verso il margine destro.

Per fare riferimento al nome di una variabile o di una colonna in un'altra istruzione BLOCK, usare la sintassi seguente:

nomeblocco::colonna | nome-variabile

Istruzione PAGE HEADER del modello di rapporto

Questa istruzione di layout inserisce informazioni nella parte superiore di ogni pagina del rapporto.

Sintassi

Per sintassi si intendono le regole che governano la scrittura delle istruzioni in un linguaggio di programmazione. Di seguito è riportata la struttura di una stringa con PAGE HEADER:

```
PAGE HEADER {parametri}
```

Parametri

Ad eccezione del fatto che non è possibile usare i nomi di colonne e variabili, i parametri per questa istruzioni sono gli stessi per FOOTER. Per un elenco e una spiegazione dei parametri validi per questa istruzione, vedere [Istruzione PAGE FOOTER del modello di rapporto](#) (a pagina 429).

Esempio

```
PAGE HEADER {  
  Data del rapporto: [CD>  
  Ora del rapporto: [CT>  
}
```

Commenti

Le intestazioni di pagina vengono stampate nella parte superiore di ogni pagina del rapporto. Possono essere definite in qualsiasi punto all'interno del file del modello del rapporto ma non possono essere incluse all'interno di un'istruzione BLOCK.

Il contenuto di un campo occupa esattamente lo spazio racchiuso tra le parentesi quadre. Qualsiasi carattere in più viene troncato. Tuttavia, è possibile chiudere un campo con una parentesi angolare di chiusura (>) per permettere di espandere il campo in tutta la sua lunghezza verso il margine destro.

Per fare riferimento al nome di una variabile o di una colonna in un'altra istruzione BLOCK, usare la sintassi seguente:

```
nomeblocco::colonna | nome-variabile
```

Istruzioni PRINT del modello di rapporto

Questa istruzione di layout inserisce i dati in una sezione dei dati del reporting.

Sintassi

Per sintassi si intendono le regole che governano la scrittura delle istruzioni in un linguaggio di programmazione. Di seguito è riportata la struttura di una stringa con PRINT:

```
PRINT {parametri}
```

Parametri

Per l'elenco e la spiegazione dei parametri validi per questa istruzione, vedere FOOTER.

Esempio

```
PRINT {  
[num ] [desc      ] [pr] [stat] [catgry] [asgn      ]  
}
```

Commenti

Inserire l'istruzione PRINT nel punto del reporting in cui si desidera visualizzare i dati. È possibile includere un'istruzione PRINT in un'istruzione BLOCK.

Il contenuto di un campo occupa esattamente lo spazio racchiuso tra le parentesi quadre. Qualsiasi carattere in più viene troncato. Tuttavia, è possibile chiudere un campo con una parentesi angolare di chiusura (>) per permettere di espandere il campo in tutta la sua lunghezza verso il margine destro.

Nota: se l'istruzione PRINT per una variabile MULTILINE viene delimitata da una parentesi angolare di chiusura (>), i caratteri ricoprono gli spazi per adattarsi al campo definito dalla parentesi quadra di apertura ([) e dalla parentesi angolare di chiusura (>). Se la variabile non è MULTILINE, l'uso della parentesi angolare consente di visualizzare tutti i dati sulla riga corrente indipendentemente dalla lunghezza.

Per fare riferimento al nome di una variabile o di una colonna in un'altra istruzione BLOCK, usare la sintassi seguente:

```
nomeblocco::colonna | nome-variabile
```

Personalizzazione dei rapporti Crystal Reports

Prima di visualizzare uno qualsiasi di questi rapporti, devono essere soddisfatte le condizioni seguenti:

- I rapporti Crystal Reports devono essere disponibili per il relativo selettore copiandoli nella directory Crystal: `$NX_ROOT/bopcfg/rpt`.
- Il client database deve essere in esecuzione e connesso al server database, in esecuzione sulla stessa macchina o su un'altra macchina. Se si usa un client CA Service Desk Manager per eseguire i rapporti Crystal Reports o Access, è necessario che sia installato un client database specifico e che sia stabilita la connessione con il server database.

Dopo aver creato i rapporti Crystal Reports personalizzati, effettuare le operazioni seguenti:

1. Copiare i rapporti Crystal Reports personalizzati nella directory Crystal seguente:

`$NX_ROOT/bopcfg/rpt`

2. Aggiungere i nomi file dei rapporti Crystal Reports personalizzati al file di configurazione seguente:

`crystal.cfg`

Sarà quindi possibile accedere ai rapporti Crystal Reports facendo clic su Start nella barra delle applicazioni, quindi scegliendo Segnalazione, Service Desk Reporting (Crystal Reports) dal menu CA Service Desk Manager (accessibile dal menu Programmi). Viene visualizzata la finestra Service Desk Reporting (Crystal).

Importante non è possibile aggiornare i client CA Service Desk Manager. Pertanto, se si creano e usano Crystal Reports sul server CA Service Desk Manager e si intende eseguire l'aggiornamento della versione di CA Service Desk Manager, è necessario copiare tutti i report personalizzati in un'altra posizione per non perderli. Terminato l'aggiornamento, copiare di nuovo i report nella directory Crystal `$NX_ROOT/bopcfg/rpt` e modificare il file `crystal.config` per renderli accessibili al selettore dei report.

Capitolo 7: Inserimento dati in CA CMDB

Questa sezione contiene i seguenti argomenti:

[Inserimento dati nel database](#) (a pagina 433)
[Modalità di inserimento dati nel database con GRLoader](#) (a pagina 433)
[Componenti di dati Federation Adapter](#) (a pagina 434)
[Glossario di inserimento dei dati](#) (a pagina 435)
[Creazione di un nome fonte dati](#) (a pagina 435)
[Modalità di importazione dei dati mediante ADT](#) (a pagina 436)
[Federation Adapters](#) (a pagina 443)

Inserimento dati nel database

L'inserimento in CA CMDB degli elementi di configurazione e delle relazioni presenti nella propria infrastruttura IT è parte integrante di un utilizzo efficiente dell'applicazione. È possibile inserire manualmente dati in CA CMDB mediante l'editor degli elementi di configurazione incorporato oppure importando elementi da altri strumenti di gestione degli asset.

Nota: per informazioni sull'editor degli elementi di configurazione, vedere la *Guida in linea*.

Modalità di inserimento dati nel database con GRLoader

L'inserimento di dati nel database mediante il caricamento di elementi di configurazione e di relazioni è un processo costituito da più passaggi, illustrati di seguito:

1. I dati di input che contengono informazioni sugli elementi della configurazione e delle corrispondenti relazioni vengono convertiti in XML.
2. Il programma GRLoader di CA CMDB utilizza i dati XML come input.
3. GRLoader carica i dati nel database.

Nota: per informazioni su GRLoader, consultare la *Guida di riferimento tecnico CA CMDB*.

4. CA CMDB contiene ADT, che consente di convertire i dati dal loro formato nativo nel corretto formato XML. Inoltre, CA CMDB include diversi Federation Adapters che utilizzano funzioni ADT.

Ulteriori informazioni:

[Avvio del server ADT ed esecuzione dello script](#) (a pagina 441)

[Utilizzare iGRLoader per importare i dati](#) (a pagina 442)

Componenti di dati Federation Adapter

Un Federation Adapter è costituito da un componente di definizione dati e da un componente di mapping dei dati.

Definizione dati

Descrive i metadati per i dati di input e di output. I metadati specificano la posizione dei dati di input o output, le modalità di accesso agli stessi e i campi in essi contenuti.

Mapping dei dati

Esegue il mapping dei campi nei campi di input ai campi di output XML. L'output del Federation Adapter è un documento XML situato nel supporto di archiviazione.

Input per Federation Adapters

È possibile utilizzare un'origine dati ODBC, un file XML o un file flat come origine per l'input nei Federation Adapters. Utilizzare ad esempio i formati seguenti per le origini dei dati di input:

- Database Oracle
- Database Ingres
- Database Microsoft Access
- Fogli di calcolo Excel
- Database DB2 MVS
- Database DBASE
- Database AS/400
- Database UDB
- File CSV (Valori separati da virgola, Comma Separated Value)
- File di testo

Nota: i nomi dei campi nel documento XML non corrispondono esattamente ai nomi dei campi nel modello di oggetti di CA CMDB. Associare i campi nei dati di input ai campi nei dati di output, quindi trasformare tali dati in base alle proprie esigenze. ADT offre una funzionalità di mapping che consente di spostare i dati dall'origine alla destinazione.

Glossario di inserimento dei dati

Programma ADT

Un *programma ADT* è una rappresentazione grafica dei mapping di dati e delle relazioni tra tabelle.

Script ADT

Uno *script ADT* è una rappresentazione di testo di un programma ADT.

Script ADT compilato

Uno *script ADT compilato* è una versione eseguibile di uno script ADT, archiviata nelle tabelle IDB all'interno dell'MDB.

Mapping grafico

Il *Mapping grafico* è un componente ADT che riguarda principalmente la modalità di spostamento dei dati dalla tabella di input nella tabella di output. Consente di creare uno script che verrà letto dal gestore script.

GRLoader

GRLoader è un programma che consente la lettura di elementi di configurazione e di relazione nei documenti XML e il caricamento di dati nelle tabelle MDB.

IDB

IDB è un set di tabelle del "database interno" di ADT all'interno del database MDB.

MDB

MDB è un database che contiene tutti i dati CA presenti in tutti i prodotti.

Profilo

Un *profilo* viene specificato nel Mapping grafico, per ogni tabella di input o di output. Per informazioni dettagliate sui dati da immettere nel profilo, consultare la guida all'interfaccia ADT appropriata.

Script Manager (Gestione script)

Script Manager è un componente ADT responsabile della gestione di profili e script.

Creazione di un nome fonte dati

Per utilizzare l'origine dati Generic ODBC di ADT, è possibile creare un nome DSN (Database Source Name) contenente le informazioni su uno specifico database per il driver ODBC.

Per creare un nome DSN

1. Dal menu Start selezionare Impostazioni, Pannello di controllo, Strumenti di amministrazione, Origini dati ODBC.

Viene visualizzata la finestra di dialogo Amministratore origine dati ODBC.

2. Fare clic su Aggiungi e selezionare il driver che supporta l'origine dei dati nella scheda DSN di sistema.
3. Fare clic su Fine.
Viene visualizzata una finestra di dialogo che consente di specificare un nome fonte dati ed altre informazioni relative all'installazione. L'aspetto della finestra di dialogo dipende dal driver selezionato.
4. Completare i campi in base al driver selezionato e fare clic su OK.
5. Per un database SQL Server 2005, selezionare SQL Native Client e fare clic su Fine.
6. Continuare seguendo le istruzioni visualizzate.
7. Accertarsi che l'opzione Esegui traduzione per dati carattere sia selezionata e fare clic su Fine.
Nota: in genere, in questa finestra di dialogo non è necessaria alcuna modifica.
8. Fare clic su Test fonte dati per verificare la connettività del database.
Al termine della verifica, fare clic su OK.
Il nome fonte dati è stato creato.

Modalità di importazione dei dati mediante ADT

Nella procedura seguente viene descritto come utilizzare ADT per inserire elementi della configurazione in CA CMDB.

1. Aprire il Mapper ADT.
2. Impostare la tabella di input.
3. Impostare il file di dati di destinazione.
4. Generare lo script.
5. Impostare i profili mediante Script Manager
6. Avviare il server ADT ed eseguire lo script.
7. Utilizzare GRLoader per importare i dati.

La fonte delle informazioni relative agli elementi di configurazione può essere un foglio di calcolo di Microsoft Excel, ad esempio un documento situato nella directory seguente:

```
<root>\cmdb\data\federationAdapters\cidata.xls
```

<root> specifica la posizione predefinita:

- c:\programmi\ca\CA CMDB per un'installazione standard
- c:\programmi\ca\servicedesk per un'installazione integrata

Aprire il Mapper ADT.

Per importare i dati degli elementi di configurazione, utilizzare il Mapper ADT ed individuare un programma esistente che soddisfa i requisiti di importazione.

Per aprire il Mapper ADT

1. Dal menu Start scegliere Programmi, CA, Advantage Data Transformer, Mapper.

Viene avviato il Mapper Advantage Data Transformer e visualizzata la pagina di connessione all'archivio metadati.

2. Completare i seguenti campi e fare clic su OK:

Seleziona nome fonte dati di IDB

Consente di specificare il nome fonte dati (DSN) che era stato creato durante l'installazione di ADT.

Immetti id utente

Specifica l'ID utente amministratore ADT, infopump.

Immetti password

Specifica la password indicata durante l'installazione di ADT.

Viene visualizzata la pagina Sfoglia archivio metadati.

3. Fare doppio clic sul file contenente il programma che si desidera eseguire. In questo caso, selezionare load_ci_from_xls. Questo file è l'adapter per il caricamento dei dati degli elementi della configurazione da un foglio di calcolo Excel.

Viene visualizzata una pagina contenente i pannelli che consentono di muovere i dati dalla tabella di input (a sinistra) alla tabella di output (a destra).

Importante I dati vengono spostati campo per campo dalla tabella di input (a sinistra) alla tabella di output (a destra). Le linee che collegano le due tabelle rappresentano i mapping dei campi tra le tabelle.

4. (Facoltativo) Fare clic con il pulsante destro del mouse sulla barra del titolo della tabella di output e scegliere "Colonne filtro" per selezionare solo i campi attivamente mappati dal programma.

Viene visualizzato un elenco semplificato.

Nel riquadro a sinistra sono elencati gli elementi presenti nel file fonte di input. Il riquadro destro elenca gli elementi del file di output. L'output per tutti i Federation Adapters è un file XML. Questo file è utilizzato come input nel programma GRLoader di CA CMDB.

5. (Facoltativo) Fare clic con il pulsante destro del mouse sulla barra del titolo a sinistra e scegliere Tabella di destinazione per convertire una tabella da un'origine di input in un'origine di output. Se l'opzione Tabella di destinazione è selezionata, la tabella è definita come tabella di output.

Importante Tutti i mapping dei campi vengono eliminati quando si converte una tabella in o da una tabella di destinazione. Durante la creazione di una tabella, identificarla o meno come tabella di destinazione in modo da non perdere il lavoro eseguito.

Impostazione della tabella di input

Impostare e verificare la definizione della tabella di input. Il Profilo associato alle Proprietà tabella contiene le definizioni necessarie ad accedere ai dati. Tali definizioni specificano il tipo di dati, la posizione dei dati e i parametri di protezione.

Per impostare la tabella di input

1. Nella pagina Mapper ADT, fare clic con il pulsante destro del mouse sul riquadro sinistro e selezionare Proprietà.
Verranno visualizzate le proprietà del file fonte di input.
2. Fare clic sulla scheda Profilo.
Viene visualizzata la pagina Selezionare profilo.
3. Specificare o selezionare un nome profilo. È possibile fare clic sul pulsante ellisse (...) alla destra del nome del profilo per selezionare un profilo.
Vengono visualizzate le specifiche del profilo.
4. Completare i campi della pagina.

Importante Creare un ODBC DSN e modificare il profilo prima di impostare la tabella di input. Creare profili aggiuntivi se necessario. In un ambiente ODBC, è necessario un DSN e un profilo per ogni database.

5. Fare clic su OK.
La pagina Selezionare profilo viene chiusa.
6. Fare clic su OK.
La pagina Proprietà tabella viene chiusa.
La tabella di input è viene impostata.

Ulteriori informazioni:

[Creazione di un nome fonte dati](#) (a pagina 435)

Impostazione del file di dati di destinazione

Impostare e verificare il file di dati di destinazione (un file XML).

Per impostare il file di dati di destinazione

1. Nella pagina Mapper ADT, fare clic con il pulsante destro del mouse sulla barra del titolo del riquadro destro, denominato Tutti, e selezionare Proprietà.
Viene visualizzata la pagina Proprietà.
2. Fare clic sulla scheda Profilo.
La pagina Proprietà visualizza un profilo adatto all'output XML.
3. Fare clic sulla scheda Informazioni sul file.
La posizione di destinazione per il file di output XML è specificata nel campo Nome file.
I Federation Adapters creano la posizione predefinita seguente per i file XML:

```
<root>\cmdb\data\userdata
```
4. (Facoltativo) Sostituire la posizione predefinita. Selezionare Specificare il nome specifico dell'istanza, fare clic su Sfoglia e passare alla posizione in cui si desidera salvare il file di dati di destinazione.
5. Fare clic su OK.
Il file di dati di destinazione è stato preparato.

Impostazione di profili mediante Script Manager

Il componente Script Manager di ADT ha i ruoli seguenti.

- Consente di gestire gli script e i profili di ADT
- Consente di modificare o creare profili da Script Manager
- Consente di eseguire script dall'ambiente di Script Manager

Importante L'Editor profili utilizzato per impostare i profili visualizza le stesse schede e gli stessi campi di input, a prescindere dal tipo di interfaccia. Per alcune interfacce sono validi solo determinati campi di immissione. Per determinare i campi appropriati per ogni tipo di interfaccia, consultare la Guida all'interfaccia ADT appropriata. L'immissione delle informazioni di configurazione per un campo di immissione non applicabile a un adapter può dare luogo a errori durante l'esecuzione dello script. Ad esempio, per profili con tipo di interfaccia Generic ODBC, impostare il campo Seleziona tipo di server nella scheda Server/Database su ODBC DSN. Tuttavia, non immettere dati nei campi Selezionare database o Immettere informazioni di connessione/modulo.

Per impostare i profili mediante Script Manager

1. Dal menu Start, selezionare Programmi, CA, Advantage, Data Transformer, Script Manager.
Verrà visualizzato Script Manager.
2. Fare doppio clic su CMDB_FederationAdapters.
Una pagina visualizza i profili ADT che vengono distribuiti con CA CMDB.
3. Fare doppio clic su cmdb_profile_xls, quindi fare clic sulla scheda Interfaccia.
Viene visualizzato l'Editor profili.
4. Qualora possibile, selezionare l'interfaccia Generic ODBC anziché l'interfaccia specifica del database.
5. Fare clic sulla scheda Server/Database e verificare che il campo Selezionare server sia impostato sul nome della connessione ODBC definita nel Profilo della tabella di input. Se l'ODBC DSN non esiste, crearne uno.
L'impostazione del Profilo è terminata.

Ulteriori informazioni:

[Creazione di un nome fonte dati](#) (a pagina 435)

Generazione dello script

Prima di eseguire un Federation Adapter o un programma ADT, generare uno script. Gli script e i profili a essi associati costituiscono gli elementi di base dei programmi visivi creati nel mapper.

Per generare uno script

1. Nella pagina Mapper ADT fare clic con il pulsante destro del mouse in un punto dello spazio compreso tra i file di input e di output, quindi scegliere Generate Script (Genera script).

Nota: la generazione di uno script dal Mapper ADT non compila automaticamente lo script. È necessario compilare lo script utilizzando ADT Script Manager.

2. Verificare la presenza di eventuali messaggi di errore visualizzati nell'angolo inferiore destro della pagina all'interno della pagina di output.

Ulteriori informazioni:

[Avvio del server ADT ed esecuzione dello script](#) (a pagina 441)

Avvio del server ADT ed esecuzione dello script

Avviare il server ADT ed eseguire lo script di importazione per creare un documento XML.

Nota: per installare il server ADT come servizio di Windows durante l'installazione e la configurazione, iniziare dal passaggio 3.

Per avviare il server ADT ed eseguire lo script di importazione

1. Dal menu Start, selezionare Programmi, CA, Advantage, Data Transformer, Server.
Viene avviato il server, che richiede ID utente e password.
2. Immettere l'ID utente e la password creati in Configura ADT.
Viene visualizzata la pagina Mapper ADT.
3. Nella pagina Mapper ADT, selezionare Strumenti, Script Manager.
ADT Script Manager viene avviato.

4. Fare clic con il pulsante destro del mouse sullo script creato in Impostazione della tabella di input e selezionare Compila.
5. Al termine della compilazione dello script, fare di nuovo clic con il pulsante destro del mouse sullo script e selezionare Esegui.
Viene eseguito lo script e creato il documento XML.
6. Aprire il file XML in Internet Explorer o Notepad e verificarne il contenuto.

Nota: Consultare Impostazione del file di dati di destinazione per il nome e la posizione del file XML.

Utilizzare iGRLoader per importare i dati

Importare i dati utilizzando il programma GRLoader fornito con CA Service Desk Manager, che crea elementi della configurazione basati sui dati del file XML creato in Avvio del server ADT ed esecuzione dello script).

Per utilizzare GRLoader per importare i dati

1. Selezionare Esegui dal menu Start.
2. Digitare cmd.

Viene visualizzata una finestra del prompt dei comandi DOS.

3. Immettere il seguente comando:

```
Grloader -u <username> -p <password> -s http://<cmdb_servername>:8080  
-i <xml_document>
```

GRLoader crea gli elementi della configurazione utilizzando i dati contenuti nel file XML. Se vengono rilevati degli errori nel corso di questo processo, verrà creato un file di errori in cui saranno elencati gli elementi della configurazione che non è stato possibile importare e il motivo.

L'importazione di GRLoader è completata.

4. Avviare CA CMDB e verificare che i dati di elementi della configurazione siano stati inseriti correttamente.
5. Avviare CMDB Visualizer per verificare che i dati di relazione siano stati inseriti correttamente.

I dati vengono importati e controllati.

Nota: per ulteriori informazioni su GRLoader, vedere la *Guida di riferimento tecnico CA CMDB*.

Federation Adapters

CA CMDB include i Federation Adapters seguenti:

Load_ci_from_xls

Consente di caricare qualsiasi famiglia di elementi di configurazione da un foglio di calcolo di Excel.

Load_generic_template

Consente di caricare qualsiasi famiglia di elementi di configurazione da qualsiasi origine dati.

Load_hardware_server

Consente di caricare gli elementi di configurazione della famiglia Hardware Server nell'MDB.

Load_relations_from_xls

Consente di caricare una tabella di relazioni tra gli elementi di configurazione da un foglio di calcolo di Excel.

Load_SMS_from_view

Consente di caricare dati Microsoft Systems Management Server (SMS) da una vista creata nel database di origine.

Load_UAM_from_view

Consente di caricare dati di gestione asset da una vista creata nell'MDB di origine.

Prerequisiti per l'esecuzione di un Federation Adapter

Verificare che i valori dei parametri seguenti siano impostati correttamente prima di eseguire un Federation Adapter di CA Service Desk Manager:

- Per ogni database o foglio di calcolo esiste un ODBC DSN.
- Esiste un profilo per ogni database/foglio di calcolo. Per un'interfaccia Generic ODBC, specificare quanto segue:
 - Server: DSN
 - Informazioni di accesso (se presenti)
 - Interfaccia: Generic ODBC
- Per ogni tabella di database, è specificato il profilo corretto nella finestra di dialogo Proprietà.

- Per ogni file di output XML, specificare quanto segue nella finestra di dialogo Proprietà.
 - Il profilo XML corretto nella scheda Profilo.
 - Il nome del file di output corretto nella scheda File.
- Lo script viene generato all'interno del Mapper ADT.
- Lo script viene compilato all'interno di ADT Script Manager.
- Viene avviato il server ADT.

Nota: per altre interfacce potrebbero essere applicabili parametri differenti. Per ulteriori informazioni, consultare la documentazione relativa all'interfaccia ADT.

Elenco di controllo dei Federation Adapter di CA Service Desk Manager

Prima di utilizzare ADT per eseguire un Federation Adapter di CA CMDB, verificare quanto segue:

- La proprietà "Visualizza output nella console" del programma sia selezionata.
- Solo per i fogli di calcolo verificare quanto segue:
 - Tutti i dati dei fogli di calcolo siano alfabetici
 - Le date siano formattate come stringhe (giustificate a sinistra)
 - I numeri siano formattati come stringhe di caratteri (giustificate a sinistra)
 - Nei nomi delle colonne non siano presenti spazi incorporati né vengano utilizzate parole chiave come DESC
- Per ogni database o foglio di calcolo esista un ODBC DSN.
- Nelle proprietà e/o nel profilo di ogni tabella del database di input sia specificato il nome corretto del profilo.
- Esiste un profilo per ogni database/foglio di calcolo. Per un'interfaccia Generic ODBC, specificare quanto segue:
 - Server: DSN
 - Informazioni di accesso (se disponibili)
 - Interfaccia: Generic ODBC

Nota: per istruzioni sull'utilizzo di altre interfacce di database, consultare le guide all'interfaccia di ADT.

- Per ogni file di output XML, verificare quanto segue:
 - Nelle proprietà o nel profilo sia specificato il profilo XML
 - Nelle informazioni sulle proprietà o sul file sia specificato il nome corretto del file di output
- In Graphical Mapper venga generato e compilato lo script.
- Il server ADT venga avviato.
- Il servizio CA Service Desk Manager Server venga avviato.

Dopo aver verificato tutti gli elementi precedenti, procedere nel modo seguente:

- Eseguire lo script da Script Manager (aggiornare la visualizzazione per visualizzare i programmi appena generati).
- Consultare il messaggio relativo all'avvio dello script, alle righe lette e all'arresto dello script nella console del server.
- Verificare la presenza di errori nei messaggi di registro della console.
- Aprire il file XML mediante un editor XML o Internet Explorer.
- Eseguire GRLoader per importare elementi di configurazione e relazioni.

Assegnazioni classi e famiglie

Applicare uno schema di classificazione a ogni elemento di configurazione. Tale schema comporta l'assegnazione degli attributi seguenti a ogni elemento di configurazione:

- Famiglia—Una raccolta di elementi della configurazione con attributi simili
- La classe—Un sottoinsieme di elementi della configurazione nell'ambito di una stessa famiglia

Le assegnazioni possono essere create nelle modalità seguenti:

- Inserire i dati del produttore che identificano la famiglia e la classe per ciascun asset hardware.
- Per famiglia e classe includere valori non vuoti nelle rispettive colonne del file di input.

GRLoader non consente di importare elementi di configurazione caricati la cui famiglia e classe non possano essere risolti in una famiglia e una classe esistenti.

Mapping dei dati fonte

È possibile importare le informazioni relative agli elementi della configurazione da più tipi di origini dati. Il foglio di calcolo `cidata.xls` in CA Service Desk Manager contiene un esempio di fonte dati. Tale foglio contiene i mapping di ciascuna delle tabelle di input specifiche di una famiglia elencate nel file.

Caricamento di elementi della configurazione da un foglio di calcolo Excel

La possibilità di caricare informazioni sugli elementi di configurazione da un foglio di calcolo offre quanto segue:

- Un valido strumento di apprendimento per il primo utilizzo di ADT
- Un semplice modo per caricare i dati contenuti in un foglio di calcolo elaborato da terzi.

È possibile utilizzare questo adapter per importare i dati di ogni famiglia di elementi di configurazione, nonché come struttura generale per l'importazione di elementi di configurazione di qualsiasi famiglia. A meno che l'utente non abbia familiarità con la definizione di tabelle ODBC in un foglio di calcolo di Excel, copiare il file `cidata.xls` e modificarlo nel modo opportuno. Se si desidera iniziare con un foglio di calcolo nuovo o vuoto, eseguire le necessarie operazioni di inserimento/denominazione nel foglio di calcolo per definire le tabelle.

Per caricare gli elementi della configurazione mediante un foglio di calcolo Excel

1. Accedere alla seguente posizione e copiare il foglio di calcolo elettronico vuoto contenuto in CA CMDB:

`<root>\cmdb\data\federationAdapters\cidata.xls`
2. Aggiungere o rimuovere righe di dati per modificare il foglio di calcolo `cidata.xls`. Se si desidera modificare l'ordine delle colonne o rimuovere alcune colonne, utilizzare il Mapper ADT per eseguire l'analisi della nuova tabella.

Importante Tutte le celle nel foglio di calcolo elettronico devono essere formattate come Testo. Se non si riesce a formattare tutte le celle come Testo, i dati potrebbero essere danneggiati o non essere convertiti correttamente.

Nel foglio di calcolo `cidata.xls` sono presenti aree di input definite per ogni famiglia di elementi di configurazione, oltre a definizioni per le tabelle aggiuntive seguenti:

Common_attributes

Elenca gli attributi comuni inclusi in ogni famiglia, ovvero l'intersezione di attributi di ogni famiglia.

All_attributes

Elenca gli attributi inclusi in una o più famiglie, ovvero l'unione di attributi di ogni famiglia. Quando si utilizza questo adapter, inserire righe nell'area dati all_attributes definita all'interno del foglio di calcolo. Verranno caricati solo i dati contenuti nella sezione dati all_attributes. Gli altri dati verranno ignorati.

Relation

Consente la definizione delle relazioni tra gli elementi della configurazione.

Nota: predefinire alcuni valori di campo in modo che vengano accettati come input valido. Definire, ad esempio, contatti e posizioni prima che un elemento di configurazione vi faccia riferimento.

3. Salvare e chiudere il foglio di calcolo.
4. Creare un ODBC DSN nel foglio di calcolo.
5. Modificare il profilo cmdb_profile_xls in modo che faccia riferimento al DSN esistente per il Federation Adapter di CA CMDB. Specificare il nome DSN creato in precedenza nella scheda Server del profilo cmdb_profile_xls.
6. Rivedere la definizione della tabella di output nelle relative proprietà allo scopo di verificarne la destinazione.
7. Generare e compilare lo script.
8. Eseguire lo script compilato in modo da trasformare il foglio di calcolo Excel in un documento XML.
9. Eseguire la lettura del documento XML e caricarvi i dati mediante l'utilità GRLoader.

Caricamento di server hardware da un foglio di calcolo Excel

Il Federation Adapter è una versione specializzata dell'adapter load_ci_from_xls. Il programma contiene esclusivamente i campi che sono stati associati a un server hardware. Nessun altro campo viene associato.

Nel foglio di calcolo, come tabella di input viene utilizzata la tabella hardware_server invece della tabella common_attributes. Invece di utilizzare la tabella All per l'output, utilizzare la definizione della tabella HardwareServer.

Invece di inserire i dati degli elementi di configurazione nella tabella `all_attributes` del foglio di calcolo, le righe vengono inserite solo nella sezione `hardware_server`.

Nota: l'adapter carica i dati solo nella tabella `hardware_server`. Tutti gli altri dati vengono ignorati.

Tutte le altre istruzioni per il [caricamento degli elementi di configurazione da un foglio di calcolo di Excel](#) (a pagina 446) vengono seguite, modificando i nomi delle tabelle di input e di output.

Per semplicità, si consiglia di inserire gli elementi nelle colonne classe e famiglia dei dati di input. Provare ad aggiungere la trasformazione `set_hardwareServer`, nella scheda Transformation (Trasformazione), al programma di mapping.

Caricamento di relazioni da un foglio di calcolo Excel

Utilizzare il Federation Adapter per caricare le informazioni sulle relazioni nel MDB da un foglio di calcolo elettronico. Per poter formare una relazione tra gli elementi di configurazione è necessario che tali elementi siano già associati tra loro.

Verrà importato solo l'input contenuto nella tabella relazioni del foglio di calcolo `cidata.xls`.

Nota: l'utilità GRLoader ordina correttamente gli aggiornamenti dell'MDB in modo che tutti gli elementi della configurazione appartenenti allo stesso batch vengano definiti prima dell'aggiunta di relazioni. Verificare con attenzione che gli elementi di configurazione inclusi nella relazione siano descritti in modo univoco nel foglio di calcolo. Per ulteriori informazioni, fare riferimento alla sezione relativa alla riconciliazione di GRLoader. Attenersi alle istruzioni relative all'importazione di `load_cidata_from_xls`, inserendo la riga di dati nell'area delle relazioni.

Modalità di caricamento dei dati SMS Microsoft

Il Federation Adapter viene utilizzato per caricare i dati Microsoft Systems Management Server (SMS) nel MDB da un database SQL Server contenente i dati SMS. Viene creata una vista nel database fonte per selezionare dati da più tabelle e semplificare il processo di mapping dei dati. I dati SMS si trovano in un database diverso da quello contenente l'MDB.

Nota: quando si utilizza questo adapter vengono importati solo i server hardware. Se si desidera importare altri dati, creare un adapter personalizzato.

Per creare la vista, è possibile modificare nel modo appropriato ed eseguire il processo di esempio seguente:

```
<root>\cmdb\data\federationAdapters\SQL_SMS_View.sql
```

Dopo aver creato la vista contenente i dati SMS, completare le operazioni seguenti:

1. Creare un ODBC DSN nella vista. Se la struttura della vista è stata modificata, creare programmi personalizzati per associare i dati.
2. Modificare il profilo cmdb_profile_xls in modo che faccia riferimento al DSN appena creato.
3. Rivedere la definizione della tabella Hardware Server nel Mapper allo scopo di verificare la destinazione della tabella di output.
4. Eseguire lo script in modo da leggere il database SMS e trasformarlo in un documento XML.
5. Eseguire la lettura del documento XML e importarvi i dati mediante l'utilità GRLoader.

Ulteriori informazioni:

[Federation Adapter personalizzati](#) (a pagina 451)

Modalità di caricamento dei dati CA APM

L'input principale del programma CA Asset Portfolio Management (CA APM) Loader è una tabella o vista contenente un estratto dei dati CA APM da importare. Tali dati sono contenuti nella tabella di database o vista denominata CMDB_Export_Asset_Data. In alcuni casi i dati da importare nell'MDB si trovano nello stesso database della destinazione. In diverse circostanze, tuttavia, i dati da importare risiedono in un database differente, ad esempio quando si importano dati tra società consociate. In ogni caso, creare una vista nello stesso database dei dati di origine.

La vista dei dati CA APM non contiene gli attributi classe e famiglia e può provenire da un sistema con un diverso schema di classificazione. Se, ad esempio, l'origine dei dati asset è un'altra società, potrebbe essere in uso un diverso sistema di classificazione.

La tabella CA_MODEL_DEF contiene un elenco di modello, che vengono confrontati con i dati contenuti in CMDB_Export_Asset_Data. Se viene rilevata una corrispondenza, la famiglia e la classe del modello vengono assegnate all'asset in corso di importazione. Se non viene rilevata alcuna corrispondenza, definire un nuovo modello per l'asset. È consigliabile copiare le voci dalla tabella di origine CA_MODEL_DEF nell'MDB di destinazione oppure aggiornare la tabella CA_MODEL_DEF con le voci relative a tutti i marchi e i numeri di modello hardware.

Lo script SQL per la creazione di tale vista si trova nella posizione seguente:

```
<root>\cmdb\data\federationAdapters\SQL_SMS_View.sql
```

Dopo aver creato la vista, procedere come indicato di seguito:

1. Creare un ODBC DSN nel foglio di calcolo.
2. Utilizzare il Mapper/Scanner ADT per eseguire l'analisi della definizione della tabella common_attributes contenuta nel foglio di calcolo.
3. Modificare il profilo cmdb_profile_xls in modo che faccia riferimento al DSN creato in precedenza.
4. Rivedere la definizione della tabella di output allo scopo di verificare la destinazione della tabella di output.
5. Generare lo script utilizzando il Mapper ADT, quindi compilarlo in Script Manager.
6. Eseguire lo script in modo da trasformare il foglio di calcolo Excel in un documento XML.
7. Eseguire la lettura del documento XML e caricarvi i dati mediante l'utilità GRLoader.

Modalità di utilizzo del modello generico

Il modello generico viene fornito come punto di partenza per la creazione di Federation Adapters. Da solo, questo modello non è eseguibile. È possibile utilizzare questo programma per creare un elemento di configurazione o una relazione aggiungendo origini dati e mapping dei campi appropriati per importare elementi di configurazione da più famiglie contemporaneamente.

Per utilizzare il modello generico per la creazione del proprio Federation Adapter, procedere come indicato di seguito:

1. Creare un ODBC DSN nel database contenente la tabella fonte degli elementi della configurazione.
2. Analizzare la tabella di input fonte mediante il Mapper e Scanner ADT.

3. Aprire il modello generico nel Mapper ADT.
Dopo aver eseguito l'analisi della tabella fonte, è possibile includerla in un programma ADT.
4. Fare clic sulla scheda Dati e spostarsi nella tabella analizzata. Trascinare l'icona che rappresenta questa tabella nella parte superiore del programma.
5. Creare un mapping delle relazioni di campo tra la tabella di input analizzata e la tabella di output che è stata inserita dal modello. Trascinare ogni campo dalla tabella di input alla tabella di output.
6. Creare un profilo per la tabella di input.
7. Rivedere il profilo per la tabella di output.
8. Rivedere la definizione della tabella di output allo scopo di verificare la destinazione della tabella di output.
9. Eseguire lo script in modo da creare il documento XML a partire dalla tabella di input.
10. Eseguire la lettura del documento XML e caricarvi i dati mediante l'utilità GRLoader.

Federation Adapter personalizzati

Quando i dati di input non corrispondono esattamente al formato dei Federation Adapters incorporati in CA CMDB, utilizzare ADT per creare un Federation Adapter personalizzato. Questa attività viene descritta nell'esempio di accesso ai dati riportato di seguito.

Nota: Consultare i documenti ADT appropriati per ottenere dettagli precisi sulle modalità di creazione di Federation Adapters personalizzati.

Esempio: Creazione di Federation Adapters personalizzati

Nell'esempio verrà preso in considerazione un database di Microsoft Access conforme a ODBC, contenuto nel seguente file:

c:\My Documents\db1.mdb

Il file db1.mdb presenta due tabelle: la prima contenente informazioni sugli elementi di configurazione e la seconda contenente informazioni sulle relazioni tra tali elementi. Presupporre che il database contenga dati sugli elementi della configurazione in più famiglie. I dati contenuti in entrambe le tabelle verranno caricati in CA CMDB.

La seguente tabella Microsoft Access [ci : Table] descrive i dati contenenti informazioni sugli elementi della configurazione. Sono indicati i nomi delle colonne:

Nome campo	Tipo di dati
ID	AutoNumber
myname	Testo
myfamily	Testo
myclass	Testo

La seguente tabella Microsoft Access [relations : Table] descrive i dati contenenti informazioni sulle relazioni. Sono indicati i nomi delle colonne:

Nome campo	Tipo di dati
ID	AutoNumber
myprovider	Testo
myrelation	Testo
myconsumer	Testo

Capitolo 8: Utilizzo di MDR Launcher

In questo capitolo viene descritto come definire gli MDR, importare dati, eseguire il mapping degli elementi di configurazione di nuovo alla relativa origine e visualizzare dati federati per un elemento di configurazione.

Questa sezione contiene i seguenti argomenti:

[MDR Launcher](#) (a pagina 454)

[Terminologia MDR](#) (a pagina 455)

[Mapping di MDR](#) (a pagina 457)

[Avvio di MDR](#) (a pagina 457)

[Visualizzatore CMDBf](#) (a pagina 458)

[Definizione di un MDR per CA CMDB](#) (a pagina 458)

[Federazione mediante GRLoader](#) (a pagina 468)

[Associazione tra elementi della configurazione MDR ed elementi della configurazione di CA CMDB](#) (a pagina 471)

[Modalità di configurazione di MDR per visualizzatore CMDBf](#) (a pagina 473)

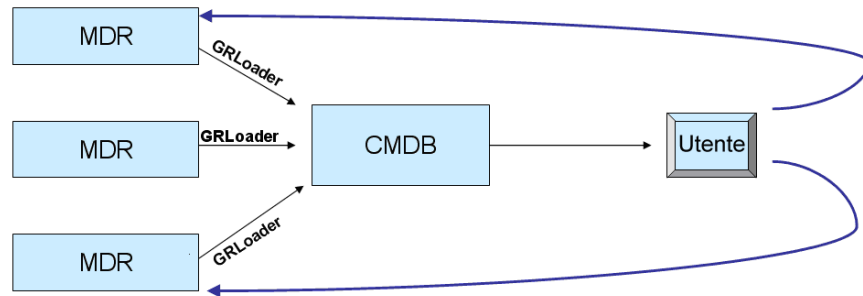
[Avvio dell'interfaccia del browser Web di MDR.](#) (a pagina 473)

[Integrazione di CA Cohesion](#) (a pagina 474)

MDR Launcher

Uno degli scopi principali dell'implementazione di CA CMDB è quello di aggregare dati da più origini dati (note come MDR). Tuttavia, un elemento della configurazione deve sempre includere un riferimento alla propria fonte MDR.

CA CMDB offre funzioni di importazione e caricamento di elementi della configurazione, nonché di associazione di questi con le relative origini. In aggiunta, utilizzando le funzioni di MDR Launcher durante la visualizzazione di un elemento della configurazione in <code>cmdb</code>, è possibile spostarsi in modo continuo nel sistema fonte degli elementi della configurazione, come illustrato nel seguente diagramma.



L'utilizzo di MDR Launcher consente di implementare un processo di gestione delle modifiche "a ciclo chiuso", come nel caso dell'esempio seguente:

1. Creazione di un record delle modifiche.
2. Implementazione delle modifiche.
3. Verifica delle modifiche tramite controllo della fonte MDR.
4. Aggiornamento del CMDB per indicare l'avvenuta modifica.

Da un punto di vista del processo di gestione dei problemi, è possibile utilizzare MDR Launcher come segue:

1. Rilevare un problema.
2. Determinare la gravità e la diffusione del problema utilizzando i dati sulle relazioni degli elementi della configurazione, al fine di individuare gli elementi interessati.
3. Determinare le possibili cause del problema eseguendo una ricerca negli elementi della configurazione fornitore.
4. Se necessario, eseguire un'analisi approfondita utilizzando le informazioni altamente dettagliate contenute nell'MDR e utilizzare quest'ultimo per intraprendere azioni correttive.

Terminologia MDR

I termini riportati di seguito sono utilizzati nell'integrazione CMDB-MDR:

Un MDR (Repository dei dati di gestione, Management Data Repository) rappresenta software o dati che contengono informazioni sulla fonte di un elemento della configurazione. Un MDR contiene in genere una quantità maggiore di dati non complessi sugli elementi della configurazione rispetto al CMDB, che contiene un sottoinsieme gestito di tali dati.

Per raggruppare gli MDR elaborati in modo analogo da CA CMDB viene utilizzata una *classe MDR* (MDR_CLASS). Esistono tre classi MDR speciali: **COHESION**, **GLOBAL** e **cmdbf**.

Un *nome MDR* (MDR_NAME) è il nome utilizzato da un MDR per fare riferimento a se stesso. Accertarsi che la combinazione dei valori `mdr_name` e `mdr_class` sia univoca all'interno dell'azienda.

Un ID asset federato (FEDERATED_ASSET_ID) è un identificatore MDR univoco per un elemento della configurazione.

Diverse famiglie di elementi della configurazione utilizzano diversi MDR rispettivi come provider di dati. Tuttavia, un singolo elemento della configurazione può essere caratterizzato da più provider di dati MDR. Ad esempio:

Famiglia elemento della configurazione	CLASSE_MDR
Contatto	sistema risorse umane
	elenco telefonico
	sistema di autenticazione single sign-on

Famiglia elemento della configurazione	CLASSE_MDR
Document	sistema di gestione documenti
Aria condizionata	sistema di gestione documenti sistema di gestione contratti sistema di controllo aria condizionata
Mainframe	sistema di gestione nastri sistema di gestione DASD sistema di gestione prestazioni pianificazione processi
Archiviazione	sistema di gestione archiviazione sistema di gestione asset
Ubicazione	sistema di gestione asset calendario dei corsi elenco ufficio
Rete	sistemi di gestione rete sistema di gestione problemi

È possibile che esistano più MDR in ogni classe MDR, e ciascun MDR può contribuire con dati in più elementi della configurazione. Un determinato elemento della configurazione può ricevere da zero a più MDR. È possibile contribuire con dati a un elemento della configurazione in modo indipendente. Ad esempio, un elemento della configurazione mainframe può contenere dati donati dal sistema di gestione dischi 1, mentre un altro elemento della configurazione mainframe può contenere dati donati dal sistema di gestione dischi 2 e dal programmatore di processi 2. CA CMDB gestisce le relazioni tra elementi della configurazione e tutti gli MDR correlati.

Mapping di MDR

Ogni MDR è dotato di un metodo di identificazione univoco degli elementi della configurazione da esso gestiti. Tali identificatori sono raramente sincronizzati negli MDR. Quando, ad esempio, si fa riferimento a uno specifico elemento di configurazione Contatto, diversi MDR possono utilizzare il numero della carta di identità, il numero di telefono, il numero di licenza o l'ID dipendente, tutti facenti riferimento alla stessa persona. Il processo di associazione di identificatori eterogenei allo stesso identificatore univoco (UUID) gestito nell'MDB viene denominato *mapping*. Il mapping viene eseguito automaticamente durante l'importazione di dati mediante GRLoader, quando l'elemento della configurazione contiene i tag `<mdr_name>` `<mdr_class>` e `<federated_asset_id>`. È possibile inoltre eseguire il mapping manualmente attraverso le funzioni di amministrazione dell'interfaccia utente. Un elemento della configurazione al quale non è stato associato alcun mapping è denominato *non federato*. Ogni elemento della configurazione è associato automaticamente a MDR globali utilizzando UUID come `federated_asset_id`.

Avvio di MDR

Quando si visualizza un elemento della configurazione utilizzando l'interfaccia utente di CA CMDB, è possibile fare clic su una serie di pulsanti per avviare direttamente un'interfaccia utente MDR. Esiste un pulsante per il mapping di MDR per l'elemento della configurazione centrale. Tale modalità di avvio è particolarmente utile quando si desidera verificare che una richiesta di cambiamento sia stata completata correttamente o per ottenere ulteriori informazioni su un elemento della configurazione quando tali dati non vengono raccolti in CMDB.

Visualizzatore CMDBf

In CA Service Desk Manager è disponibile il Visualizzatore CMDBf che consente di visualizzare i risultati della federazione di elementi della configurazione nei repository dati di gestione MDR. Da una pagina Dettagli elemento della configurazione (oppure nel menu di scelta rapida visualizzato facendo clic con il pulsante destro del mouse su un elemento della configurazione in un elenco di elementi della configurazione), fare clic su Visualizzatore CMDBf per visualizzare contemporaneamente gli attributi elemento della configurazione di CMDB federati e MDR. Nella vista federata è possibile fare clic sul pulsante Recupera per aggiornare le informazioni da qualsiasi MDR federato. Per una migliore leggibilità, i file metadata CA CMDB possono riconciliare i nomi di attributi MDR e i nomi di attributi CA CMDB.

Nota: questa funzionalità richiede repository dati di gestione MDR che supportano Query. Per configurare i risultati nella vista federata, è necessario configurare gli endpoint CMDBf MDR. Per ulteriori informazioni, consultare la *Guida all'implementazione*.

Definizione di un MDR per CA CMDB

Per poter associare un elemento di configurazione a un MDR, è necessario definire l'MDR in CA CMDB.

Per definire un nuovo provider MDR

1. Nella scheda Amministrazione passare a CA CMDB, Gestione MDR, Elenco MDR.
2. Fare clic su Crea nuovo.
Viene visualizzata la pagina Crea nuova definizione MDR.
3. Completare i campi:

Titolare

Identifica il proprietario titolare dell'MDR (se è installato Multi-Tenancy).

Nome pulsante

Consente di specificare l'etichetta del pulsante MDR da visualizzare nella pagina Dettagli elementi della configurazione. Questo nome deve essere univoco per ciascun MDR. Richiesto per "avvio in contesto" e visualizzatore CMDBf.

Nome MDR

Specifica la stringa per la corrispondenza dei dati XML inviati nel campo `mdr_name`. Sebbene sia possibile specificare qualsiasi stringa per l'MDR, viene utilizzato spesso il nome host. Tale nome, insieme a `mdr_class`, forma un nome univoco per l'MDR. Richiesto per "avvio in contesto" e visualizzatore CMDBf.

Classe MDR

Consente di specificare la classe che deve corrispondere ai dati inviati nel campo `mdr_class` nell'XML. Sebbene sia possibile specificare un nome qualsiasi, tale nome deve formare insieme al campo `mdr_name` un identificatore univoco per l'MDR. Gli MDR globali sono definiti con una classe MDR di **GLOBAL**.

- Gli MDR di CA Cohesion ACM devono specificare una classe MDR di **COHESION** con cui vengano automaticamente impostati i campi Percorso, Parametri e URL da avviare nei valori richiesti per il contesto di avvio di CA Cohesion ACM.
- Gli MDR di CA Asset Portfolio Management r11.3.4 devono specificare un nome MDR della classe APM e MDR di **GLOBAL** con cui vengano automaticamente impostati i campi Percorso, Parametri e URL da avviare nei valori richiesti per il contesto di avvio di CA Asset Portfolio Management r11.3.4.
- Gli MDR di CA APM r12.5 devono specificare un nome MDR della classe ITAM e MDR di **GLOBAL** con cui i campi Percorso, Parametri e URL da avviare vengano automaticamente impostati sui valori richiesti per il contesto di avvio di CA APM 12.5.
- Per il visualizzatore CMDBf, la classe MDR deve essere **cmdbf**.

Attivo

Indica se la definizione dell'MDR è attiva o non attiva. Le definizioni non attive dell'MDR vengono eliminate in modo logico, ma possono essere riattivate mediante l'utilità di ricerca.

Proprietario

Consente di specificare il contatto responsabile di questo MDR.

Descrizione

Consente di specificare una descrizione in testo in formato libero.

Nome host

Consente di specificare il nome host, il nome DNS o l'indirizzo IP dell'host, contenente il server Web che ospita la pagina Web da avviare. Obbligatoria per "l'avvio nel contesto".

Porta

Consente di specificare la porta TCP/IP utilizzata dal server Web dell'MDR per fornire le pagine Web. La porta 80 è quella predefinita. Obbligatoria per "l'avvio nel contesto".

Percorso

Consente di specificare la porzione dell'URL che precede il carattere punto interrogativo (?). Queste informazioni sono reperibili nella documentazione relativa a MDR.

- Per il tag `mdr_class Cohesion`, il valore viene automaticamente impostato su `"CAisd/html/cmdb_cohesion.html"` e non è possibile modificarlo.
- Per `mdr_name` di APM e `mdr_class` di "GLOBAL", il valore è impostato automaticamente su `apm/frmObject.aspx` e non può essere modificato.
- Per `mdr_name` di ITAM e `mdr_class` di "GLOBAL", il valore è impostato automaticamente su `ITAM/Pages/Asset.aspx` e non può essere modificato.

Parametri

Consente di specificare la porzione dell'URL che segue il carattere punto interrogativo (?). Per ottenere informazioni in merito, consultare la documentazione dell'MDR.

- Per il tag `mdr_class Cohesion`, il valore viene automaticamente impostato su:
`"hostname={hostname}+port={port}+family={family}+name={name}+secret={password}+federated_asset_id={federated_asset_id}"` e non è possibile modificarlo.
- Per `mdr_name` di APM e `mdr_class` di "GLOBAL", il valore è impostato automaticamente su
`ObjectID={cmdb_asset_id}&obj=11&FUNCTION=1&WinID=OBFRASSET{cmdb_asset_id}&WinContainerID=` e non può essere modificato.
- Per `mdr_name` di ITAM e `mdr_class` di "GLOBAL", il valore è impostato automaticamente su
`ParentClass=Asset&assetid={cmdb_asset_id}&TicketID={itam_ticketid}` e non può essere modificato.

Userid

Consente di specificare il nome di accesso utente MDR, se richiesto. Questo valore viene sostituito nell'URL in cui si trova il parametro {userid}. Se vuoto, il valore predefinito di userid corrisponde a chiunque abbia appena effettuato l'accesso.

Per CA Cohesion ACM, "Segreto condiviso" è il segreto utilizzato per l'accesso a CA Cohesion ACM, se richiesto. Questo valore viene sostituito nell'URL in cui si trova il parametro {password}.

Nota: per ulteriori informazioni, consultare la *Guida all'implementazione di CA Cohesion ACM*.

Segreto condiviso

Consente di specificare le informazioni condivise tra CA CMDB e l'MDR. Questo valore viene sostituito nell'URL in cui si trova il parametro {password}. Il valore degli MDR per CA Cohesion ACM deve corrispondere al valore di "com.cendura.security.oneclickauth.secret". Per ulteriori informazioni sulla creazione di un segreto condiviso, consultare il capitolo "Integrazione con CA CMDB nella *Guida all'implementazione di CA Cohesion ACM*". Richiesto per il Visualizzatore CMDBf.

Spazio nomi di CMDBf

Specifica il `federated_asset_id` che viene passato alla query come ID locale. Per CA CMDB, il valore è `http://cmdb.ca.com/r1`.

CMDBf Timeout

(Opzionale) Specifica il limite di tempo per query endpoint CMDBf. L'impostazione predefinita è dieci (10) secondi.

URL da avviare

Il valore predefinito di `http://{hostname}:{port}/{path}?{parameters}`. Per alcuni MDR, è possibile ignorare questo valore per tenere conto dei requisiti specifici degli MDR. Obbligatorio per "l'avvio nel contesto".

Per `mdr_name` di APM e `mdr_class` di GLOBAL, il valore è `http://{hostname}:{port}/{path}?{parameters}`

Per `mdr_name` di ITAM e `mdr_class` di GLOBAL, il valore è `http://{hostname}:{port}/{path}?{parameters}`

Per `mdr_class` di Cohesion il valore predefinito è `http://cmdb_hostname:cmdb_port/{path}?{parameters}`

dove:

cmdb_hostname è il nome host, nome DNS o indirizzo IP del server Web CA CMDB. Per impostazione predefinita, viene utilizzato il nome host corrente utilizzato per l'accesso al server Web CA CMDB.

porta_cmdb rappresenta la porta TCP/IP del server Web CMDB. Per impostazione predefinita, viene utilizzato il numero di porta corrente utilizzato per l'accesso al server Web CA CMDB.

Nota: se è attivato il supporto SSL per CA Cohesion ACM, è necessario impostare l'URL su:

`http://nomehost:porta/{path}?{parameters}+https=yes`

Per informazioni sull'attivazione del supporto HTTP per CA Cohesion ACM, vedere l'argomento della guida in linea di CA Cohesion ACM "Creazione di un certificato HTTP e attivazione dell'HTTP".

Endpoint CMDBf

Specifica l'endpoint Servizio query per MDR. Questa opzione è necessaria per il Visualizzatore CMDBf e per recuperare i dati MDR aggiornati. Se si utilizza CA CMDB come fornitore MDR, il valore sarà `http://cmdb_hostname:cmdb_port/axis/services/QueryPort`.

Fare clic su Salva.

Il MDR è stato definito.

Definizioni URL MDR

Il valore predefinito dell'URL da avviare è `http://{nomehost}:{porta}/{percorso}?{parametri}`. Se necessario, è possibile modificare questa espressione in modo da inserire considerazioni specifiche di MDR. L'URL è obbligatorio per l'"avvio nel contesto".

Per `mdr_name` di APM o ITAM e per `mdr_class` di "GLOBAL", il valore predefinito è:

`http://{hostname}:{port}/{path}?{parameters}`

Per il tag `mdr_class Cohesion`, il valore predefinito è:

`http://nomehost_cmdb:porta_cmdb/{path}?{parameters}`

cmdb_hostname

Specifica il nome host, il nome DNS o l'indirizzo IP del server Web di CA CMDB. Il valore predefinito è il nome dell'host corrente che accede attualmente al server Web di CA CMDB.

cmdb_port

Specifica la porta TCP/IP del server Web di CA CMDB. Il valore predefinito è il numero della porta corrente utilizzata per accedere al server Web di CA CMDB.

Se è stato abilitato il supporto SSL per CA Cohesion ACM, impostare l'URL su:

`http://nomehost:porta/{path}?{parameters}+https=yes`

Nota: per informazioni sull'abilitazione del supporto HTTPS di CA Cohesion ACM, vedere la Guida in linea di CA Cohesion ACM.

URL di avvio dell'MDR

L'URL di avvio dell'MDR ha il valore predefinito seguente:

`http://{hostname}:{port}/{path}?{parameters}`

È possibile modificare questa espressione per soddisfare aspetti specifici dell'MDR. L'URL è obbligatorio per l'"avvio nel contesto".

- Per `mdr_name` di APM o ITAM e per `mdr_class` di "GLOBAL", il valore predefinito è:

`http://{hostname}:{port}/{path}?{parameters}`

- Per il tag `mdr_class Cohesion`, il valore predefinito è:

`http://nomehost_cmdb:porta_cmdb/{path}?{parameters}`

cmdb_hostname

Nome host, nome DNS o indirizzo IP del server Web di CA CMDB. Il valore predefinito è il nome dell'host corrente che accede attualmente al server Web di CA CMDB.

cmdb_port

Porta TCP/IP del server Web di CA CMDB. Il valore predefinito è il numero della porta corrente utilizzata per accedere al server Web di CA CMDB.

Se è attivato il supporto SSL per CA Cohesion ACM, è necessario impostare l'URL su:

`http://nomehost:porta/{path}?{parameters}+https=yes`

Nota: per informazioni sull'abilitazione del supporto HTTPS di CA Cohesion ACM, vedere l'argomento sulla creazione del certificato HTTPS e l'abilitazione di HTTPS nella Guida in linea di Cohesion.

Definizione dei parametri di avvio per la sostituzione di un URL

Quando si definisce un MDR, è possibile crearne l'URL per la visualizzazione utilizzando i parametri seguenti. I valori di questi parametri vengono sostituiti con quelli appropriati in fase di esecuzione. Queste variabili devono essere specificate nei campi descritti precedentemente.

{hostname} rappresenta il nome host dell'MDR nella definizione dell'MDR.

{alarm_id} rappresenta l'indirizzo IP dell'elemento di configurazione selezionato.

{federated_asset_ID} rappresenta l'identificatore univoco dell'elemento di configurazione selezionato nell'MDR.

{cmdb_asset_id} è l>ID dell'asset per l'elemento della configurazione.

{port} rappresenta il numero di porta dell'MDR nella definizione dell'MDR.

{userid} rappresenta l>ID utente nella definizione dell'MDR. Se vuoto, il valore predefinito di userid corrisponde a chiunque abbia appena effettuato l'accesso.

{password} è il segreto condiviso nella definizione dell'MDR.

{mdr_name} rappresenta il campo mdr_name nella definizione dell'MDR.

{mdr_class} rappresenta il campo mdr_class nella definizione dell'MDR.

{class} rappresenta la classe dell'elemento di configurazione selezionato.

{family} rappresenta la famiglia dell'elemento di configurazione selezionato.

{path} rappresenta il percorso descritto nella definizione dell'MDR.

{name} rappresenta il nome dell'elemento di configurazione selezionato.

{model} è il modello dell'elemento di configurazione selezionato

{manufacturer} è il produttore dell'elemento di configurazione selezionato

{itam_ticketid} è l>ID ticket per accedere a CA APM

Esempio: avvio di un MDR

Un utente di CA CMDB sta cercando un elemento della configurazione server denominato server1, che è associato a un'applicazione sviluppata internamente, denominata Comet. Comet identifica in modo univoco il server1 come server:server1.

L'applicazione Comet è definita come MDR con le seguenti proprietà:

- Nome host: CometServer
- Porta: 80
- Percorso: index.php
- Parametri: item={federated_asset_id}
- Launch_url: http://{hostname}:{port}/{path}?{parameters}

In CA CMDB, quando l'utente seleziona il pulsante Comet nella scheda Attributi dell'elemento della configurazione server 1, viene aperta una finestra del browser Web al seguente URL:

http://CometServer:80/index.php?item=server:server1

Parametri per la sostituzione di URL

Quando si definisce un MDR, è possibile utilizzare i parametri seguenti per creare il relativo URL da visualizzare. I valori di questi parametri vengono sostituiti con quelli appropriati in fase di esecuzione. Queste variabili devono essere specificate nelle definizioni dei campi MDR.

{hostname}

Consente di specificare il nome host MDR tratto dalla definizione MDR.

{alarm_id}

Consente di specificare l'indirizzo IP dell'elemento della configurazione selezionato.

{federated_asset_ID}

Consente di specificare l'identificatore univoco dell'elemento della configurazione selezionato nell'MDR.

{cmdb_asset_id}

Consente di specificare l'ID asset per l'elemento della configurazione.

{port}

Consente di specificare il numero di porta MDR nella definizione MDR.

{userid}

Consente di specificare l'ID utente tratto nella definizione MDR. Se vuoto, il valore predefinito di userid corrisponde a chiunque abbia appena effettuato l'accesso.

{password}

Consente di specificare il segreto condiviso tratto nella definizione MDR.

{mdr_name}

Consente di specificare il mdr_name nella definizione di MDR.

{mdr_class}

Consente di specificare il mdr_class nella definizione di MDR.

{class}

Consente di specificare la classe dell'elemento della configurazione selezionato.

{family}

Consente di specificare la famiglia dell'elemento della configurazione selezionato.

{path}

Consente di specificare il percorso come descritto nella definizione di MDR.

{name}

Consente di specificare il nome dell'elemento della configurazione selezionato.

{model}

Consente di specificare il modello dell'elemento della configurazione selezionato.

{manufacturer}

Consente di specificare il produttore dell'elemento della configurazione selezionato.

Esempio: Utilizzo dei parametri per la sostituzione di URL

Un utente di CA CMDB sta cercando un elemento della configurazione server denominato server1, che è associato a un'applicazione sviluppata internamente, denominata Comet. Comet identifica in modo univoco il server1 come server:server1.

L'applicazione Comet è definita come MDR con le seguenti proprietà:

- Nome host: CometServer
- Porta: 80
- Percorso: index.php
- Parametri: item={federated_asset_id}
- Launch_url: http://{hostname}:{port}/{path}?{parameters}

In CA CMDB, quando l'utente seleziona il pulsante Comet nella scheda Attributi dell'elemento della configurazione server 1, viene aperta una finestra del browser Web al seguente URL:

`http://CometServer:80/index.php?item=server:server1`

Federazione mediante GRLoader

Quando si utilizza GRLoader, è necessario inserire i seguenti tag XML in ogni elemento della configurazione del documento XML. Questi tag si applicano a ogni famiglia MDR.

- `<mdr_name>`
- `<mdr_class>`
- `<federated_asset_id>`

Se tali informazioni non sono presenti nel documento XML, l'"avvio in contesto" non è possibile in quanto risulta impossibile determinare la fonte dell'elemento della configurazione.

Per identificare la fonte di un elemento della configurazione, è possibile modificare il documento XML prima che venga immesso in GRLoader. È possibile utilizzare un editor di testo per modificare l'XML ed eseguire un cambiamento globale oppure programmare l'esecuzione di tale operazione.

Nota: per ulteriori informazioni sull'identificazione MDR, vedere la *Guida di riferimento tecnico CA CMDB*.

Nota: CA ACM (Cohesion Application Configuration Manager) fornisce automaticamente i tag `mdr_name`, `mdr_class` e `federated_asset_id`.

Federazione di un elemento di configurazione

Se gli elementi della configurazione vengono caricati in CA CMDB prima che il corrispondente MDR sia stato definito, non verranno federati, cioè non sono ancora connessi a un MDR e non supportano ancora l'"avvio in contesto".

Per federare un elemento di configurazione

1. Definire l'MDR richiesto.
2. Eseguire una delle seguenti operazioni:
 - Inserire manualmente l'elemento della configurazione.
 - Eseguire nuovamente il report di CA Cohesion ACM che ha creato l'elemento della configurazione, specificando Consenti aggiornamento degli elementi della configurazione esistenti sul report.

Nota: Per ulteriori informazioni sui report di CA Cohesion ACM, consultare la *Guida del prodotto CA Cohesion ACM*.

3. Rieseguire GRLoader, specificando lo stesso file di input utilizzato per creare gli elementi della configurazione.

Il motore di riconciliazione di CA CMDB unisce le informazioni sull'MDR agli elementi di configurazione esistenti.

4. Creare un documento XML che descriva l'elemento della configurazione e il relativo MRD, quindi eseguire GRLoader nella modalità di aggiornamento.

Il motore di riconciliazione di CA CMDB unisce le nuove informazioni agli elementi della configurazione esistenti. L'elemento della configurazione esistente è stato federato.

Esempio: Specificare la posizione dell'elemento della configurazione

È necessario verificare che il motore di riconciliazione disponga delle informazioni necessarie per individuare l'elemento di configurazione da aggiornare. Nell'esempio seguente, sono stati rimossi i tag finali e aggiunti degli spazi per una migliore leggibilità.

```
<ci>
  <name>    server3
  <mac_address>
  <serial_number>
  <asset_num>
  <dns_name>
  <mdr_name>  mdr_one
  <mdr_class> Cohesion
</ci>
```

Definizione di più MDR in un elemento della configurazione mediante GRLoader

È possibile definire più MDR multipli in un elemento della configurazione utilizzando GRLoader.

Per definire più MDR in un singolo elemento della configurazione, il documento XML può ripetere il nodo <ci> e ogni nodo <ci> duplicato deve specificare un diverso tag mdr_name e mdr_class. In altri termini, ogni MDR può contribuire con i propri attributi in modo indipendente da qualsiasi altro MDR che contribuisce con i propri dati all'elemento della configurazione.

Esempio: Definizione di più MDR in un elemento della configurazione

Se MDR1 e MDR2 contribuiscono con i relativi dati all'elemento della configurazione del server2, il documento XML avrà il seguente aspetto. Nell'esempio riportato di seguito, sono stati rimossi i tag finali e aggiunti degli spazi per una migliore leggibilità.

```
<ci>
  <name>   server2
  <mdr_name> mdr1
  <mdr_class> Cohesion
  <diskspace> 500 gb
  <disktype> SCSI-3
</ci>
<ci>
  <name>   server2
  <mdr_name> mdr2
  <mdr_class>Service Assure
  <sla>
</ci>
```

CA CMDB riconcilia i due elementi della configurazione precedenti e associa ciascuno dei due MDR a tale elemento della configurazione singolo.

Nota: Si osservi che è possibile importare gli elementi della configurazione in una o due esecuzioni di GRLoader.

Associazione tra elementi della configurazione MDR ed elementi della configurazione di CA CMDB

Dopo aver definito manualmente un elemento della configurazione mediante l'opzione File, Nuovo elemento della configurazione... , è necessario definire manualmente l'associazione tra questo elemento della configurazione e quello contenuto nell'MDR federato. Esistono due metodi per l'associazione di un elemento della configurazione a un MDR:

- Modifica dell'elemento della configurazione.
- Utilizzo del nodo di mapping dell'elemento della configurazione federato nella scheda Amministrazione CA CMDB.

Per creare una associazione mediante la modifica dell'elemento della configurazione

1. Visualizzare la pagina dei dettagli dell'elemento della configurazione che si desidera associare a un MDR.
2. Fare clic su Modifica.
3. Visualizzare la scheda Attributi.
4. Fare clic su Aggiungi MDR.

L'elemento di configurazione viene associato all'MDR.

Per creare un'associazione mediante la pagina di mapping dell'elemento della configurazione federato

1. Fare clic sulla scheda Amministrazione CA CMDB.
2. Aprire il nodo MDR (Repository dei dati di gestione, Management data repository).
3. Selezionare il nodo del mapping dell'elemento della configurazione federato.

Viene visualizzato l'Elenco di mapping dell'elemento della configurazione federato.

4. Fare clic su Crea nuovo.

Viene visualizzata la pagina Crea nuovo mapping dell'elemento della configurazione federato per.

5. Associare l'elemento della configurazione al MDR completando i campi Mapping dell'elemento della configurazione federato:

Nome CI

Consente di specificare il nome da utilizzare per identificare l'elemento della configurazione.

ID asset federato

Consente di specificare l'identificatore di stringa utilizzato dall'MDR fonte per identificare questo elemento della configurazione.
L'identificatore è determinato dal software MDR.

Nome MDR

Consente di specificare il nome che identifica il MDR (e il relativo pulsante MDR).

Attivo

Indica se la mappatura è attiva o meno. Le mappature possono essere solo disattivate, ma non eliminate.

6. Fare clic su Salva.

Il mapping tra questo elemento della configurazione e l'elemento della configurazione del MDR federato è stato definito.

Modalità di configurazione di MDR per visualizzatore CMDBf

Per poter utilizzare il visualizzatore CMDBf, impostare i provider MDR federati in modo che puntino al servizio query CMDBf, nel modo seguente:

- Gli MDR esterni devono specificare un servizio query che possa gestire la query InstanceIdConstraint.
- È necessario che il nome pulsante, il nome MDR e la classe MDR mostrino il pulsante del visualizzatore CMDBf nella pagina dei dettagli degli elementi di configurazione.
- La classe MDR deve essere definita come **cmdbf**
- Per CA CMDB, è necessario impostare lo spazio dei nomi CMDBf su **http://cmdb.ca.com/r1**. Per altri CMDB e MDR, consultare la documentazione appropriata.
- Il timeout è facoltativo. L'impostazione predefinita è dieci (10) secondi.
- Per visualizzare un pulsante Recupera funzionante nella vista federata, è necessario definire il punto finale CMDBf, l'ID utente e il segreto condiviso.

Nota: è possibile impostare un sistema CA CMDB esistente come provider CMDBf specificando il punto finale CMDBf

"http://servername:port/axis/services/QueryPort" dove:

- hostname è il computer in cui è installato CA CMDB (nome computer o localhost).
- port è la porta in cui è configurato CA CMDB.

Avvio dell'interfaccia del browser Web di MDR.

Dopo aver creato un mapping tra un elemento della configurazione e un MDR, viene automaticamente inserito un pulsante nella scheda Attributi. Se più MDR sono stati associati a questo elemento della configurazione, verranno visualizzati più pulsanti.

Quando si fa clic su un pulsante MDR, verrà aperta una nuova pagina contenente l'URL MDR completamente sostituito, definito nell'MDR.

Esempio: Avvio di CA Cohesion

Quando un elemento della configurazione è stato associato correttamente al suo MDR, viene visualizzato un pulsante Cohesion nella scheda Attributi. Se nella scheda Attributi non compare alcun pulsante, controllare il mapping per l'elemento della configurazione visualizzato. Accertarsi che esista un mapping per questo elemento della configurazione e che l'MDR di destinazione disponga di un URL avviabile. Se si fa clic sul pulsante per avviare l'MDR, verrà aperta una nuova finestra all'URL di destinazione per avviare CA Cohesion.

Integrazione di CA Cohesion

Prendere in considerazione le seguenti informazioni quando si integra CA Cohesion ACM in CA CMDB:

- Integrazione di Cohesion in CA CMDB

Nota: Per informazioni sull'integrazione Cohesion-CA CMDB, consultate la *Guida all'implementazione di CA Cohesion ACM*.

- Importazione di elementi della configurazione da un MDR Cohesion

Nota: per informazioni sulle modalità di importazione degli elementi di configurazione da un MDR Cohesion, vedere la Guida in linea disponibile nella scheda CA Cohesion ACM, Report, Modelli report.

- Avvio in contesto per MDR Cohesion

Per il funzionamento ottimale dell'integrazione di avvio in contesto con CA ACM (Cohesion Application Configuration Manager), si consiglia di utilizzare la scheda Amministrazione CA CMDB per definire gli MDR Cohesion *prima* di eseguire il report CMDB Cohesion.

Nota: poiché CA ACM (Cohesion Application Configuration Manager) non supporta un ID asset federato univoco per gli elementi della configurazione NIC o File System, Cohesion non supporta MDR Launcher per gli elementi della configurazione NIC o File System. Di conseguenza, un elemento della configurazione NIC o File System basato su Cohesion non contiene un pulsante di avvio MDR, neanche se è stato impostato correttamente.

Capitolo 9: Gestione dei servizi Web

Importante Per ulteriori informazioni sui servizi Web, consultare la Guida all'implementazione di CA Service Desk Manager.

Questa sezione contiene i seguenti argomenti:

- [Gestione dei servizi Web](#) (a pagina 475)
- [Componenti di CA Service Desk Manager](#) (a pagina 476)
- [Suggerimenti per i client dei servizi Web](#) (a pagina 476)
- [Configurazione dei servizi Web](#) (a pagina 479)
- [Sicurezza dei servizi Web](#) (a pagina 481)
- [Gestione degli errori](#) (a pagina 483)
- [Installazione dei servizi Web](#) (a pagina 487)
- [Specifiche esterne](#) (a pagina 487)
- [Oggetti](#) (a pagina 508)
- [ITIL, metodologia](#) (a pagina 514)
- [Utilizzo dei servizi Web](#) (a pagina 516)

Gestione dei servizi Web

I *servizi Web* sono un set di standard per lo scambio di dati che abilita le comunicazioni tra più prodotti, anche se sono in ambienti completamente differenti. È analogo alla navigazione sul Web con un PC, grazie alla quale è possibile accedere a tutti i siti Web indipendentemente dalla piattaforma utilizzata, ad esempio Solaris, AIX, Windows e così via. Allo stesso modo, i servizi Web consentono alle applicazioni di comunicare tra loro utilizzando il protocollo HTTP su vari server, a prescindere dalla piattaforma. Ad esempio, un'applicazione di Microsoft Office può comunicare con un programma presente su un server UNIX e una JSP (Java Server Page) può accedere a un server di Windows. Si tratta di comunicazioni a piattaforma neutra che consentono di eseguire integrazioni estremamente efficaci.

I servizi Web sfruttano questa tecnologia, permettendo a quasi qualsiasi prodotto di accedere a CA Service Desk Manager e a Gestione delle informazioni. I client dei servizi Web possono creare ticket, aggiornare gli asset, eseguire ricerche nell'archivio della conoscenza e altro ancora.

Componenti di CA Service Desk Manager

I file di installazione per questa versione del servizio Web J2EE vengono installati al momento dell'installazione di CA Service Desk Manager e di Gestione delle informazioni e possono trovarsi nella directory seguente:

```
<NX_ROOT>/sdk/websvc/R11
```

I file di installazione per i servizi Web J2EE compatibili con le versioni precedenti si trovano nella directory seguente:

```
<NX_ROOT>/sdk/websvc/60
```

dove <NX_ROOT> è il percorso di installazione principale per CA Service Desk Manager.

Suggerimenti per i client dei servizi Web

Un'applicazione del client Java esemplificativa per i servizi Web nella cartella *samples* dell'installazione di CA Service Desk Manager aiuta gli sviluppatori con lo sviluppo di applicazioni client di servizi web.

Molti metodi dei servizi Web richiedono degli array come parametri di input. Ad esempio, il metodo `createIssue()` consente l'utilizzo di un array vuoto per il parametro 'propertyValues'. Talvolta, questi array sono opzionali ma il servizio richiede il passaggio di un array vuoto. Per utilizzare Visual Studio .NET per accedere ai servizi Web, si consiglia di specificare un array vuoto con uno degli array seguenti:

Linguaggio C#

```
String[] emptyArray = new string[0];
```

Visual Basic .NET:

```
Dim emptyArray As String() = {}
```

Java

```
ArrayOfString agent = new ArrayOfString();  
attr.setString(new String[0]);  
ArrayOfString è una classe proprietaria.
```

emptyArray può essere quindi passato ai parametri dell'array che accettano gli array vuoti.

Nota: i servizi Web di CA Service Desk Manager utilizzano l'implementazione Apache degli standard stabiliti dal World Wide Web Consortium (W3C). Idealmente, un client di qualsiasi tipo di ambiente operativo dovrebbe essere in grado di accedere ai servizi; tuttavia, le implementazioni dei fornitori possono variare. Molti ambienti di programmazione forniscono uno strumento per generare classi proxy da una descrizione WSDL (Web Services Description Language).

Ulteriori informazioni:

[Client Java](#) (a pagina 477)

Client Java

TableOfContents.doc in \$NX_ROOT/samples/sdk/websvc elenca vari programmi Java di esempio.

Ciascun programma di esempio contiene note su come può essere compilato ed eseguito utilizzando i file di script run_java_test.bat.txt (Windows) e run_java_test.sh.txt (UNIX). Questi script dimostrano come utilizzare org.apache.axis.wsdl.WSDL2Java per generare i file stub lato cliente dei servizi Web di CA Service Desk Manager.

Il parametro -w è richiesto per generare correttamente i file stub quando si usa Axis 1.4. L'esecuzione di WSDL2Java come mostrato genera i file stub nella sottodirectory com/ca/www/UnicenterServicePlus/ServiceDesk. Vengono creati i seguenti file:

- ArrayOfInt.java
- ArrayOfString.java
- ListResult.java
- USD_WebService.java
- USD_WebServiceLocator.java
- USD_WebServiceSoap.java

■ USD_WebServiceSoapSoapBindingStub.java.

Importare queste classi con la seguente istruzione:

```
import com.ca.www.UnicenterServicePlus.ServiceDesk.*;
```

Molti metodi di servizi Web hanno parametri del tipo `ArrayOfString`, una classe proprietaria. Per esempio, per `attrVals` del metodo `createRequest()`, `propertyValues` e parametri di attributi sono tutti parametri `ArrayOfString`.

Per impostare i valori in una variabile `ArrayOfString`, instanziare la variabile e utilizzare `setString()` come segue:

```
ArrayOfString attrVals = new ArrayOfString();  
attrVals.setString(new String[]{"cliente", customerHandle, "descrizione", "testo descrizione"});
```

Per impostarlo come vuoto

```
attrVals.setString(new String[0]);
```

Utilizzare una variabile del tipo `ListResult`, un'altra classe proprietaria, come valore restituito dai metodi `List`: `doQuery()`, `getRelatedList()`, `getNotificationsForContact()`, `getPendingChangeTaskListForContact()` e `getPendingIssueTaskListForContact()`. Una `ListResult` contiene gli elementi `listHandle` e `listLength`, che possono essere recuperati utilizzando `getListHandle()` e `getListLength()` come mostrato in questo esempio:

```
ListResult doQueryResult = new ListResult();  
doQueryResult = USPSD.doQuery(sid, "iss", "active = 1");  
int listHandle = doQueryResult.getListHandle();  
int listLength = doQueryResult.getListLength();
```

Il metodo `getListValues()` utilizza `listHandle`, recuperando i valori da un sottoinsieme dell'elenco.

Il parametro `Handles` del metodo `freeListHandles()` è un `ArrayOfInt`, un'altra classe proprietaria. Richiamare `freeListHandles()` utilizzando `listHandle` preso da `ListResult`:

```
ArrayOfInt handleList = new ArrayOfInt();  
handleList.setInteger(new java.lang.Integer []{ new java.lang.Integer(listHandle) });  
USPSD.freeListHandles(sid, handleList);
```

Alcuni metodi hanno parametri pass by reference del tipo `javax.xml.rpc.holders.StringHolder`. Per esempio, `createRequest()` ha due parametri di questo tipo, `NewRequestHandle` e `NewRequestNumber`.

```
StringHolder NewRequestNumber = new StringHolder();
StringHolder NewRequestHandle = new StringHolder();
Risultato stringa;
result = USPSD.createRequest(sid, creatorHandle, attrVals, propertyValues, template, attributes,
NewRequestHandle, NewRequestNumber);
```

Request's handle e reference number (ref_num) possono essere ottenuti da `NewRequestHandle.value` e `NewRequestNumber.value` rispettivamente.

Configurazione dei servizi Web

I servizi Web di CA Service Desk Manager possono essere configurati con apposite voci in speciali file di configurazione Web. I nomi e le descrizioni delle opzioni di configurazione si possono riepilogare come segue:

Nome opzione	Descrizione
<code>design_mode_stubs</code>	Imposta il servizio Web sulla 'modalità progetto' (solo CA Service Desk Manager).
<code>require_secure_logon</code>	Richiede il richiamo dei metodi Web <code>login()</code> e <code>loginService()</code> con un protocollo protetto, ad esempio <code>https</code> .
<code>require_secure_connection</code>	Richiede il richiamo di tutti i metodi Web con un protocollo protetto.
<code>disable_user_logon</code>	Disabilita entrambi i metodi Web <code>login()</code> e <code>loginService()</code> . In questo modo, solo il metodo <code>loginServiceManaged()</code> è disponibile per l'accesso.

Nota: è possibile impostare i parametri di configurazione nel file `deploy.wsdd`. Per Unicenter Service Desk r11.0, questo file si trova nella sottodirectory: `<NX_ROOT>/sdk/websvc/R11`. Per la precedente versione GA 6.0, il file si trova nella sottodirectory seguente: `<NX_ROOT>/sdk/websvc/60`. Si consiglia di creare una copia di backup di uno dei file prima di apportarvi qualsiasi cambiamento.

CA Service Desk Manager ha aumentato la protezione all'integrità del server Tomcat sul quale è in esecuzione controllando la lunghezza dei valori attribuito passati ai metodi Web Service. Per impostazione predefinita, i richiami web service restituiranno un Axis Fault se la lunghezza di un valore attribuito è superiore a 900.000 byte.

I seguenti parametri vengono impostati nel file `deploy.wsdd`.

- **`fatal_max_string_length`**. Imposta la lunghezza del valore attributo più lungo accettato da un metodo web service.

Impostazione predefinita: 900.000 byte

- **`validate_parameters`**. Stabilisce se avviene un controllo della lunghezza del valore attributo. Impostare su 0 per disabilitare la convalida.

Impostazione predefinita: 1 (attivo)

- **`exception_methods`**. Mostra un elenco delimitato da virgola di metodi Web Service esclusi dalla convalida della lunghezza del valore attributo.

Ulteriori informazioni:

[Ridistribuzione dei servizi Web](#) (a pagina 480)

Ridistribuzione dei servizi Web

Le nuove impostazioni di configurazione verranno applicate alla nuova ridistribuzione dei servizi Web CA Service Desk Manager. Completare i seguenti passaggi per ridistribuire i servizi Web:

1. Aprire un prompt dei comandi e impostare la variabile di ambiente `CLASSPATH` in modo che includa i file Axis jar necessari. Tali file si trovano in `<NX_ROOT>/java/lib`. Ad esempio, per impostare la posizione in Windows, utilizzare la variabile di ambiente seguente:

```
set AXISHOME=%NX_ROOT%\javallib
set classpath=
%AXISHOME%\axis.jar;%AXISHOME%\jaxrpc.jar;%AXISHOME%\saaj.jar;%AXISHOME%\commons-logging.jar;%AXISHOME%\commons-discovery.jar;%AXISHOME%\wsdl4j.jar;%AXISHOME%\log4j-1.2.8.jar;%classpath%
```

2. Accedere alla directory `<NX_ROOT>/sdk/websvc/R11` (oppure `<NX_ROOT>/sdk/websvc/60` per i servizi Web della precedente versione GA 6.0) ed eseguire i comandi seguenti:

```
java org.apache.axis.client.AdminClient undeploy.wsdd
java org.apache.axis.client.AdminClient deploy.wsdd
```


3. Riavviare Tomcat riavviando il servizio CA Service Desk Manager. Per evitare di arrestare l'intero sistema CA Service Desk Manager è possibile riavviare Tomcat semplicemente utilizzando i comandi seguenti:

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

A questo punto i servizi Web sono ridistribuiti. È possibile verificare l'effettiva ridistribuzione dei servizi visualizzando la pagina contenente l'elenco di tutti i servizi Axis all'URL seguente:

`http://<nomeserver>:<porta>/axis/services`

Nota: l'URL esatto dipende dalle impostazioni di installazione.

Sicurezza dei servizi Web

Ci sono diversi importanti fattori sulla protezione da tenere in considerazione quando si distribuiscono i servizi Web. Quando si utilizza il protocollo HTTP, la configurazione predefinita non è protetta. Se la rete utilizza questo protocollo, tutte le informazioni in formato di testo semplice trasmesse nelle chiamate dei servizi Web tra i client e i server non sono protette. Oltre ai dati delle applicazioni (ad esempio, le descrizioni dei ticket e i nomi dei contatti), tra le informazioni non protette sono inclusi anche i SID (Service Session Identifier) delle sessioni dei servizi Web e, a seconda del metodo di accesso utilizzato dal servizio Web, le password. Questa sezione è destinata in particolar modo agli amministratori che si occupano della distribuzione dei servizi Web. Qualora sia necessario eseguire procedure di configurazione aggiuntive ai livelli di applicazione e di rete al fine di proteggere l'ambiente dei servizi Web, si consiglia di leggere con estrema attenzione le informazioni che seguono.

Importante la configurazione dei servizi Web che utilizza il protocollo HTTP non è protetta e pertanto è vulnerabile alle minacce dal mondo esterno. Tali minacce possono includere i tentativi di lettura delle password, il session-fixation, lo spionaggio dei dati e altro ancora.

Ci sono tre fattori principali relativi alla protezione da tenere in considerazione quando si distribuiscono i servizi Web:

- Quali schemi di autenticazione per l'accesso (al livello di applicazione) deve supportare la distribuzione?
- Quali altre funzioni di protezione al livello di rete richiede la distribuzione?
- In che modo devono essere applicati questi requisiti tramite le opzioni di configurazione dei servizi Web?

Le risposte a queste domande sono descritte di seguito.

- **Schemi di autenticazione livello applicazione servizi Web**—Per accedere ai servizi Web, un'applicazione client di servizi Web dev'essere autenticata con l'applicazione servizi Web. I servizi Web offrono due schemi di autenticazione per l'accesso. Il primo schema è rappresentato dal nome utente e dalla password; il secondo dalla tecnologia PKI (Public Key Infrastructure, infrastruttura a chiave pubblica). Nei servizi Web entrambi gli schemi lavorano a stretto contatto con il controllo dell'accesso e con il componente di gestione dell'accesso, utilizzando infatti la stessa norma di accesso. L'autenticazione per l'accesso e la gestione dell'accesso rappresentano le funzioni di protezione più importanti per i servizi Web.

L'autenticazione che si basa sui metodi nome utente e password può essere disabilitata utilizzando il comando di configurazione della protezione seguente:

```
disable_user_logon
```

Prima di abilitare questa opzione, l'amministratore deve determinare se ciascun client dei servizi Web, per cui un'organizzazione richiede l'accesso ai servizi Web, può effettivamente fornire il supporto per il metodo di autenticazione alternativo, ovvero il metodo di accesso basato su PKI. Il vantaggio principale della tecnologia PKI sta nel fatto che le applicazioni client dei servizi Web non richiedono la *gestione* degli account degli utenti di sistema, ovvero la gestione, la custodia e la trasmissione delle password.

- **Configurazione di sicurezza livello di rete**—Tenere presente che in entrambi gli schemi di autenticazione, quello basato sui nomi utente/password e quello basato sulla tecnologia PKI, gli ID di sessione restituiti dal metodo di accesso specifico (e tutte le altre informazioni correlate) vengono trasmessi in formato di testo semplice se si utilizza il protocollo HTTP. Inoltre, se si utilizza lo schema di autenticazione basato sul nome utente/password, la password viene inviata non protetta (in formato di testo semplice) dall'applicazione client ai servizi Web. Durante lo sviluppo del prodotto, W3C (World Wide Web Consortium) non aveva stabilito standard per la protezione dei servizi Web. Di conseguenza, la protezione dei servizi Web non è una funzionalità utilizzata da queste implementazioni di servizi per garantire un ambiente protetto. Si consiglia invece l'uso di protocolli di protezione al livello di trasporto punto a punto (SSL/TLS) e altri meccanismi di protezione al livello di rete (ad esempio, IPSec) per proteggere le trasmissioni di dati in formato di testo semplice per lo scambio delle informazioni sull'autenticazione al livello di applicazione e le trasmissioni degli ID di sessione e dei dati correlati.

Importante Si consiglia l'uso del protocollo SSL (o https) quando si distribuiscono i servizi Web per proteggere gli scambi delle informazioni relative all'autenticazione al livello di applicazione e le trasmissioni degli ID di sessione e dei dati correlati.

- **Configurazione servizi Web**—Per applicare la protezione delle comunicazioni (basate su protocollo) al livello dell'applicazione dei servizi Web, sono disponibili i due comandi di configurazione della protezione seguenti:

`require_secure_logon`

Questa funzione di protezione richiede l'uso del protocollo SSL (o https) per il richiamo dei metodi `Login()` e `LoginService()`. Questa funzione fornisce un metodo pratico per proteggere il nome utente e la password e allo stesso tempo evita il sovraccarico del protocollo SSL per ciò che riguarda gli altri aspetti dei servizi Web.

Importante se si utilizza il comando `require_secure_logon`, l'applicazione dei servizi Web non confermerà che la protezione al livello di protocollo per le comunicazioni è applicata per metodi diversi da `Login()` e `LoginService()`. A meno che non vengano implementate altre precauzioni, è possibile che altri metodi per i servizi Web vengano richiamati senza misure di protezione, rendendo i sistemi più vulnerabili e quindi più esposti alle minacce dal mondo esterno.

`require_secure_connection`

Questa funzione di protezione richiede l'utilizzo del protocollo SSL per accedere a qualsiasi parte del servizio Web. Se è richiesto il protocollo https ma non viene utilizzato, viene restituito un errore SOAP con codice `UDS_SECURE_CHANNEL_REQUIRED`.

Nota: per ulteriori informazioni sulle modalità di configurazione del protocollo SSL, consultare la documentazione del contenitore servlet J2EE.

Ulteriori informazioni:

[Specifiche esterne](#) (a pagina 487)

Gestione degli errori

Se si verifica un errore nell'utilizzo di un metodo dei servizi Web, viene restituito un errore SOAP. L'errore SOAP è il metodo standard per la restituzione delle informazioni di eccezione per i servizi Web.

Il messaggio di errore contiene gli elementi standardizzati `<Message>` e `<Code>` ma quello che fornisce le maggiori informazioni è l'elemento `<Detail>`. L'elemento `<Detail>` contiene a sua volta gli elementi `<ErrorCode>` e `<ErrorMessage>`. L'elemento `<ErrorCode>` restituisce un codice di errore numerale specifico del prodotto CA Service Desk Manager o Gestione delle informazioni. L'elemento `<ErrorMessage>` contiene una stringa in lingua inglese che descrive gli errori. Gli elementi `<ErrorMessage>` aiutano i sviluppatori nelle loro attività e gli utenti con messaggi sempre adeguati.

Ad esempio, di seguito viene illustrato un errore SOAP quando al metodo getObjectValues() di CA Service Desk Manager viene passato un parametro non valido:

```
<soap:Fault>
  <faultcode>soap:Client</faultcode>
  <faultstring>Error on fetch with attribute list:persistent_id,first_name,last_nameParamErrorHere</faultstring>
  <detail>

    <ErrorCode>1001</ErrorCode>

    <ErrorMessage> Errore caricamento con elenco attributi: persistent_id,first_name,last_nameParamErrorHere
  </ErrorMessage>
  </detail>
</soap:Fault>
```

Se si utilizza un client creato con il codice gestito di Microsoft .NET, una chiamata non valida al metodo dei servizi Web genera un'eccezione "SOAPException". Tutti gli errori annullano l'operazione richiamata.

In alcuni casi, gli errori possono essere scritti dall'esecutore di servlet e pertanto visualizzati nei registri di tale esecutore. In altri casi, le informazioni sugli errori vengono scritte nei registri CA Service Desk Manager. Questi registri si trovano nelle sottodirectory seguenti:

- nella sottodirectory /bopcfg/www/CATALINA_BASE/logs dell'installazione CA Service Desk Manager
- nella sottodirectory /log dell'installazione CA Service Desk Manager e in tutti i registri con prefisso "stdlog"

Nota: si consiglia di monitorare costantemente questi registri poiché il server potrebbe registrare gli errori senza comunicarlo ai servizi Web CA Service Desk Manager.

Errori di blocco

Gli oggetti CA Service Desk Manager sono bloccati durante gli aggiornamenti. I metodi che aggiornano gli oggetti, ad esempio updateObject() o transfer(), possono restituire il codice di errore di blocco seguente:

UDS_LOCK_ERR

Questo codice indica che un altro utente sta aggiornando il record. Spesso, l'handle dell'utente che causa il blocco viene restituito nell'elemento ErrorMessage.

TimeOut

L'elaborazione di un metodo può richiedere molto tempo se il server CA Service Desk Manager è sottoposto a un carico eccessivo di lavoro. Raramente, è possibile che la restituzione di un metodo non avvenga mai a causa della mancata risposta da parte di un processo separato oppure per il verificarsi di altri errori. Per evitare blocchi eccessivamente lunghi, il timeout di ogni metodo dei servizi Web si verifica dopo uno specifico numero di secondi. Il timeout dei metodi dei servizi Web è un timeout del server CA Service Desk Manager e *non* del server Web, della rete e così via.

Quando si verifica un timeout, viene restituito il codice di errore seguente:

UDS_TIMEOUT_ERR

L'operazione non viene annullata. Il server potrebbe aver già ricevuto la richiesta e la elaborerà regolarmente, sebbene più lentamente. Questo tipo di problema può verificarsi quando si usa il metodo *doSelect()* per recuperare svariate migliaia di record.

Nota: per informazioni sul metodo *doSelect*, vedere la *Guida di riferimento tecnico di CA Service Desk Manager*.

Nota: dopo il riavvio del server applicazioni J2EE, la prima volta che si accede ai servizi Web, l'accesso avviene con un leggero ritardo. Questo avviene poiché è in corso l'inizializzazione dell'applicazione, il caricamento delle DLL, delle librerie e così via e si verifica solo con la prima chiamata al metodo dei servizi Web. Tutte le chiamate successive avvengono molto più rapidamente.

Codici di errore

La tabella seguente riporta i valori possibili per il valore <ErrorCode> in un errore SOAP restituito da una chiamata ai servizi Web:

Nome errore	Valore	Descrizione
UDS_OK	0	Esito positivo.
UDS_FAILURE	1	Errore generale, controllare i registri degli errori.
UDS_BAD_PARAM	1000	A un metodo è stato passato un parametro non valido. Questo errore si verifica se manca un parametro obbligatorio, se viene passato un parametro errato oppure se è stato utilizzato un valore non valido.
UDS_INTERNAL_ERR	1001	Segnala la presenza di un errore interno. Una descrizione dell'errore è presente nell'array di

Nome errore	Valore	Descrizione
		restituzione e nei registri di sistema.
UDS_LOCK_ERR	1002	È stato tentato l'aggiornamento di un oggetto bloccato da un altro utente o processo. Solitamente, l'ID del contatto responsabile del blocco dell'oggetto viene incluso ai dati di restituzione.
UDS_UPDATE_ERR	1003	Si è verificato un errore durante l'aggiornamento di un oggetto. Accertarsi che tutti gli attributi necessari siano stati impostati e controllare il registro di sistema.
UDS_CREATION_ERR	1004	Si è verificato un errore durante la creazione di un nuovo oggetto. Accertarsi che tutti gli attributi necessari siano stati impostati e controllare il registro di sistema.
UDS_NOT_FOUND	1005	Un metodo di ricerca non è riuscito a trovare delle corrispondenze oppure l'oggetto specificato. Questo può avvenire se viene passato un handle non valido a un metodo.
UDS_SESSION_TIMEOUT	1006	Si è verificato il timeout del metodo corrente, è possibile che il server CA Service Desk Manager sia sovraccarico oppure che il metodo stesso sia errato.
UDS_SERVER_GONE	1007	La connessione al server di CA Service Desk Manager si è interrotta, i metodi UDS non funzioneranno più e non sono più disponibili tutti i riferimenti dell'elenco.
UDS_FETCH_ERR	1008	Si è verificato un errore durante il recupero dei dati dell'elenco.
UDS_BAD_SESSION	1010	È stato utilizzato un SID non valido.
UDS_CNTXT_TIMEOUT	1011	Si è verificato il timeout del SID.
UDS_SECURE_CHANNEL_REQUIRED	1012	I servizi Web (o un metodo di servizio Web) richiede un canale sicuro (per esempio: SSL) per l'accesso, ma si sta utilizzando un canale non sicuro.
UDS_SECURITY_VIOLATION	1013	L'operazione che si è tentato di eseguire viola la protezione di CA Service Desk Manager ed è stata annullata.
UDS_OVER_POLICY_LIMIT	3002	La richiesta che si è tentato di eseguire è stata rifiutata poiché supera il limite definito nella norma.

Installazione dei servizi Web

I servizi Web sono installati durante l'installazione di CA Service Desk Manager sia per il server primario che per quello secondario. Per permettere ai client di servizi Web di utilizzare un URL su un server secondario, occorre aggiungere un motore Web al server secondario.

Nota: per informazioni sull'aggiunta e la configurazione dei Web Director e dei motori Web, vedere la *Guida all'amministrazione di CA Service Desk Manager*.

Per impostazione predefinita, i servizi Web utilizzeranno la Gestione oggetti del server primario chiamato *domsrvr*. Per utilizzare qualsiasi altro gestore oggetti, impostare ed installare l'opzione Gestione opzioni *webservice_domsrvr*. Gestione oggetti può trovarsi su un server primario o secondario.

Nota: per informazioni sull'impostazione e sull'installazione dell'opzione *webservice_domsrvr*, vedere la *Guida in linea*.

Modalità di attivazione di Design-Time

I servizi Web CA Service Desk Manager mettono a disposizione degli sviluppatori una funzione di configurazione degli stub dei metodi. Quando questa funzione viene attivata, i servizi Web ignorano il server di CA Service Desk Manager e restituiscono i dati simulati per le chiamate dei metodi, quindi le chiamate ai servizi Web possono essere effettuate senza che il server di CA Service Desk Manager sia in esecuzione.

Per attivare design-time nella versione Java, seguire questi passaggi:

1. Modificare *deploy.wsdd* per decommentare le sezioni per "design_mode_stubs".
2. Occorre invertire la distribuzione e ridistribuire il server.
3. Riavviare il server di applicazioni.

La funzione design-time è attivata.

Nota: la funzione di design-time è valida solo per i metodi dei servizi Web CA Service Desk Manager.

Specifiche esterne

CA Service Desk Manager consente di specificare l'autenticazione dell'accesso utente e le funzionalità disponibili per la gestione e il controllo degli accessi.

Autenticazione per l'accesso utente

I servizi Web CA Service Desk Manager offrono due schemi di autenticazione per l'accesso. Sono associati alle nuove funzioni di controllo di accesso e di gestione, che utilizza una norma de accesso.

Nome utente/Password

Verifica il nome utente e la password, come descritto nella prima versione del prodotto.

Tecnologia PKI (Public Key Infrastructure, infrastruttura a chiave pubblica)

Verifica che la persona che richiede l'accesso disponga di una specifica chiave privata.

Importante se si decide di utilizzare un'applicazione che abbia accesso a questa versione dei servizi Web di CA Service Desk Manager, si consiglia di definire prima una norma di accesso del servizio Web, completo del relativo valore di codice in CA Service Desk Manager. Una norma di accesso predefinita con un codice norma DEFAULT è disponibile dopo l'installazione e la configurazione di CA Service Desk Manager.

Ulteriori informazioni:

[Definizione di una norma di accesso](#) (a pagina 498)

Autenticazione Nome utente/Password

Se si decide di utilizzare il tipo di autenticazione per l'accesso Nome utente/Password, l'applicazione dell'utente deve richiamare uno dei due metodi dei servizi Web seguenti per accedere ai servizi Web CA Service Desk Manager.

Nota: l'utente collegato specificato nel parametro username (non il contatto proxy specificato nel criterio) è responsabile delle attività intraprese in una sessione. All'utente collegato viene applicata la protezione del gruppo funzioni e la partizione dati.

login (username, password)

Questo metodo viene fornito per la compatibilità con le versioni precedenti, in cui l'autenticazione per l'accesso viene eseguita sul nome utente e sulla password specificati. Un SID (session ID, ID sessione) viene restituito solo se l'accesso viene autenticato. Tutte le successive chiamate ai servizi Web devono includere il SID. La norma di accesso predefinita viene quindi applicata a tutti i successivi accessi ai servizi Web a cui è associato il SID.

Il nome utente e la password sono campi obbligatori in cui è necessario immettere informazioni in formato di testo semplice.

loginService (nome_utente, password, norma)

Questo metodo è simile alla funzione di accesso precedente in cui l'autenticazione per l'accesso viene eseguita sul nome utente e sulla password specificati. Viene restituito un SID solo se l'accesso viene autenticato. Tuttavia, per controllare e gestire i successivi accessi ai servizi Web, viene applicata una norma di accesso specifica, indicata dal terzo parametro. Se per il parametro norma non viene specificato alcun valore, viene applicata automaticamente la norma predefinita.

Il nome utente e la password sono campi obbligatori in cui è necessario immettere informazioni in formato di testo semplice. Il parametro Norma è obbligatorio e deve essere specificato in formato di testo semplice, tuttavia è possibile lasciarlo vuoto. Utilizzare il codice di norma definito in una norma.

La modalità di validazione dell'accesso dipende dall'oggetto del contatto *tipo di accesso* assegnato. L'oggetto tipo di accesso si trova in CA Service Desk Manager ed imposta il tipo validazione. È possibile utilizzare il prodotto per visualizzare il record Tipo accesso ed utilizzare anche il metodo Web `getAccessTypeForContact()` per recuperare le informazioni sull'oggetto Tipo accesso.

Nota: per ulteriori informazioni sui tipi di accesso, consultare la *Guida per l'amministratore*.

Autenticazione PKI (Public Key Infrastructure, infrastruttura a chiave pubblica)

Se si decide di utilizzare l'autenticazione PKI, tenere presente che il contenuto della richiesta di accesso viene crittografato con una chiave privata e che può essere decifrato solo utilizzando la chiave pubblica corrispondente. La risposta alla richiesta di accesso viene restituita in formato di testo semplice.

In genere, a ogni applicazione che accede ai servizi Web di CA Service Desk Manager viene assegnata una norma. I servizi Web CA Service Desk Manager memorizzano le informazioni dettagliate su un criterio, insieme alla chiave pubblica di un certificato digitale. Un'applicazione, ad esempio quella relativa al titolare della norma, utilizza la chiave privata del certificato digitale e il codice norma (identificativo della norma) per generare una richiesta di accesso.

loginServiceManaged (norma, norma_crittografata)

I servizi Web CA Service Desk Manager eseguono l'autenticazione utente individuando il criterio tramite il codice di criterio in testo semplice, recuperando la chiave pubblica del titolare del criterio associata al codice di criterio, decifrando il codice di criterio crittografato, associando il contenuto decifrato al codice di criterio e quindi aprendo una sessione con il server di backend. Viene restituito il SID (ID sessione) in formato di testo semplice e può essere utilizzato per il richiamo successivo di altri metodi. Solo il titolare del criterio dispone della chiave privata corrispondente alla chiave pubblica associata del criterio memorizzata in CA Service Desk Manager.

Tutte le successive chiamate ai servizi Web devono includere il SID restituito. Il contatto proxy specificato nella norma è responsabile di tutte le attività dei servizi Web avviati in questa sessione. Al contatto proxy viene applicata la protezione del gruppo funzioni e la partizione dati.

Importante il parametro norma_crittografata deve essere in formato di testo BASE64. L'applicazione dell'utente deve eseguire la conversione dal formato binario.

Il campo Norma è obbligatorio. Quando viene definito, utilizzare il codice di norma in formato di testo semplice, come definito in una norma. Il parametro norma_crittografata (la firma digitale del codice di norma crittografata con la chiave privata del titolare della norma) è obbligatorio. Quando si definisce il parametro norma_crittografata, utilizzare l'algoritmo SHA1 con RSA per ottenere la firma digitale.

Implementazione di loginServiceManaged in Java

Di seguito viene mostrato come generare Certificati e quindi utilizzarli per accedere ai servizi Web di CA Service Desk Manager.

Nell'esempio seguente il processo di accesso viene completato utilizzando il certificato di CA Service Desk Manager e vengono quindi eseguite due chiamate ai servizi Web comuni. La chiamata al metodo dei servizi Web getBopsid() consente di ottenere un token collegato a un utente specifico. Il token può essere utilizzato per accedere all'interfaccia Web di CA Service Desk Manager come utente collegato senza che venga richiesta una password. Ciò permette l'integrazione trasparente tra applicazioni diverse.

Importante il token BOPSID generato scade dopo 30 secondi e pertanto deve essere utilizzato subito.

Nota: utilizzare lo strumento AXIS noto come WSDL2Java per generare le classi stub necessarie. È possibile scaricarlo dal sito <http://ws.apache.org/>.

Importante quando si utilizza la versione 1.4 dello strumento AXIS si verifica una questione nota. Per ulteriori informazioni, vedere le *Note di rilascio*.

Implementazione di loginServiceManaged in Java

1. Avviare il servizio CA Service Desk Manager.
2. Eseguire `pdm_pki -p DEFAULT`.

Nella directory corrente viene creato il file `DEFAULT.p12`. In questa norma la password è uguale al nome della norma, in questo caso `DEFAULT`.

Nota: questo comando aggiunge anche la chiave pubblica del certificato al campo `pub_key` (attributo `public_key`) nella tabella/oggetto `sapolicy`.

3. Accedere a CA Service Desk Manager e selezionare la scheda Amministrazione.

Passare a Criterio servizi Web, Criteri.

Viene visualizzato l'Elenco norme di accesso servizi Web.

4. Fare clic su `DEFAULT`.

Viene visualizzata la pagina Aggiorna norma di accesso servizi Web.

5. Completare il campo Contatto Proxy (in questo esempio `ServiceDesk`) e controllare che il campo Con chiave del record della norma `DEFAULT` sia impostato su "Sì".

6. Copiare `DEFAULT.p12` (dalla directory dove viene eseguito il comando `pdm_pki`), il file JSP denominato `pkilogin.jsp` e il file HTML denominato `pkilogin.htm` (dalla directory `$NX_ROOT\samples\sdk\websvc\java\test1_pki`) nella seguente directory:
`$NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\axis`

7. Aprire il modulo HTML dalla directory di axis, ad esempio
`http://localhost:8080/axis/pkilogin.htm`

Completare i campi appropriati.

Nota: il campo Directory identifica la posizione del file del certificato. Modificare il percorso con la posizione corretta.

8. Fare clic su Log me in!

Viene visualizzata la pagina dei risultati.

9. Fare clic sull'URL con BOPSID.

Importante click this immediately! Il BOPSID presenta un token con una durata limitata pari a circa 30 secondi.

Il formato di un URL che utilizza un BOPSID è:

`http://<nome server>:<porta>/CAisd/pdmweb.exe?BOPSID=<valore BOPSID>`

Nota: per utilizzare il metodo `loginServiceManaged` per un programma client Java in esecuzione su AIX, potrebbe essere necessario sostituire una coppia di file di criteri di sicurezza in `JAVA_HOME`. Visitare il sito <http://www.ibm.com> e cercare "developerworks java technology security information AIX". Nel documento "developerWorks : Java technology : Security" seguire il link a "IBM SDK Policy files". Scaricare i file dei criteri senza restrizioni, `local_policy.jar` e `US_export_policy.jar`. Utilizzare questi file per sostituire i file originali nella directory `JAVA_HOME/lib/security`.

Configurazione per l'autenticazione PKI

Per configurare l'autenticazione PKI, per prima cosa è necessario creare un criterio di accesso. Il processo richiesto è il seguente:

Creare un criterio di accesso

L'amministratore esegue questa attività utilizzando il prodotto (solo interfaccia Web) e, durante il processo, deve assegnare un codice di testo univoco a ciascun criterio di accesso.

Ottenere un certificato digitale con una coppia di chiavi pubblica/privata e associarlo al criterio di accesso

Per l'autenticazione per l'accesso PKI, l'applicazione dell'utente deve ottenere il certificato digitale contenente la coppia di chiavi pubblica e privata. Un amministratore può ottenere il certificato digitale tramite l'Autorità di certificazione (CA) di terzi oppure tramite i prodotti di protezione che supportano i certificati digitali. CA Service Desk Manager fornisce inoltre un'utilità per il server in grado di generare un certificato digitale. Questa utilità si trova nella directory <NX_ROOT>/bin nel modo seguente:

```
pdm_pki -p codice_norma [-f file_certificato] [-i] [-h]
```

-p

Identifica un codice di criterio univoco.

-f

Consente all'utilità di sostituire la chiave pubblica esistente con una nuova chiave pubblica.

-i

Carica la chiave pubblica archiviata in un certificato X509 V3.

-h

Visualizza le informazioni della Guida sulla finestra della riga di comando.

Se si ottiene un certificato digitale tramite terze parti, CA o prodotti di protezione, importarlo nella stessa ubicazione in cui si trova il server CA Service Desk Manager e associarlo a un criterio di accesso.

L'amministratore dell'applicazione dell'utente deve ottenere un file del certificato digitale che includa il contenuto di un certificato X509 V3 in formato DER/ASN.1.

Inoltre, il certificato deve contenere solo la chiave pubblica della coppia di chiavi pubblica/privata. Utilizzando l'opzione -i, l'amministratore richiama l'utilità pdm_pki che consente di caricare il certificato. L'utilità carica il certificato, estrae la chiave pubblica, la converte in formato di testo BASE64 e lo salva con il criterio di accesso specificato dal codice di criterio.

Quando un certificato digitale viene generato dall'utilità `pdm_pki`, l'amministratore richiama il comando in CA Service Desk Manager senza utilizzare l'opzione `-l`. L'utilità genera quindi una coppia di chiavi pubblica e privata (le chiavi sono di tipo RSA a 1024 bit). La chiave pubblica viene convertita in formato testo BASE64 e viene memorizzata insieme al criterio di accesso specificato dal codice di criterio. Viene creato anche un certificato X509 V3 per contenere la chiave pubblica insieme alle altre informazioni necessarie (la fase di passaggio predefinita viene impostata come il codice criterio). Il certificato X509 V3 viene infine unito alla chiave privata in un certificato trasferibile standard in formato PKCS12. Viene quindi salvato in un file chiamato *policy_code.p12* in base al codice di norma fornito. Questo file può essere quindi esportato sui client.

Nota: se un criterio di accesso è già stato associato a una chiave pubblica di un certificato, gli utenti devono specificare l'opzione `-f` durante la chiamata al comando `pdm_pki` per sovrascrivere la chiave pubblica esistente con una nuova.

Ulteriori informazioni:

[Definizione di una norma di accesso](#) (a pagina 498)

Accesso ai servizi Web

Di seguito viene descritto il flusso del processo di accesso ai servizi Web configurati con l'autenticazione PKI:

Processo	Descrizione
Caricare il certificato digitale ed estrarre la chiave privata	Il certificato digitale deve essere archiviato dall'utente in un supporto di archiviazione protetto, dal quale può essere recuperato e utilizzato per accedere ai servizi Web. Esempi di supporti di memorizzazione protetti includono: ■ Archivio certificati di Windows. ■ Archivio certificati di Java (gestito dall'utilità Java Keytool). ■ Archivio certificati (creato da altri prodotti di protezione CA). Un'applicazione utente deve essere in grado di caricare il certificato digitale ed estrarre la chiave privata utilizzando le API appropriate, in base all'ambiente utilizzato dall'utente.
Creare una firma digitale del codice di criterio in formato di testo semplice con la	Dopo aver estratto la chiave privata dal certificato digitale, questa può essere utilizzata

Processo	Descrizione
chiave privata	per generare una firma digitale del codice di criterio. La creazione di una firma digitale crittografa un digest di un testo con una chiave privata. L'algoritmo con classificazione (digest) deve essere SHA1 standard e l'algoritmo di crittografia deve essere RSA. La firma digitale binaria deve inoltre essere convertita in formato di testo BASE64 per poter essere utilizzata per accedere ai servizi Web. In base all'ambiente utilizzato dall'utente, per memorizzare queste informazioni è necessario utilizzare le chiamate API appropriate.
Eeguire la chiamata al servizio Web	Un'applicazione utente deve richiamare il metodo <code>loginServiceManaged()</code> dei servizi Web insieme al codice di criterio in formato di testo semplice e alla firma digitale in formato di testo BASE64 del codice criterio.
Ottenere il SID restituito	Se la richiesta di accesso viene autenticata, viene automaticamente restituito un SID in formato di testo semplice.

Una volta generato, il SID stabilisce un collegamento tra una sessione del servizio Web e un criterio di accesso. Con questo SID l'applicazione utente può richiamare altri metodi dei servizi Web e tutti i relativi accessi ai servizi Web vengono controllati e gestiti da tale criterio di accesso.

Sessione e autorizzazione

Una validazione corretta restituisce un SID associato al nome utente validazione, sia che si tratti del nome utente fornito per l'accesso o del contatto proxy specificato in una norma. Grazie a questo processo, a ogni utente di CA Service Desk Manager vengono assegnati diritti di protezione che possono essere utilizzati nell'applicazione del servizio Web.

Ad esempio, un utente può lavorare con una partizione dati che limita le richieste che possono essere visualizzate. Quando l'utente utilizza un SID per ottenere informazioni sulle richieste, il sistema CA Service Desk Manager verifica che la partizione dati venga applicata.

Viene applicata anche la protezione del gruppo funzioni. Ad esempio, un utente potrebbe non avere accesso al gruppo funzioni di Call Manager. Non è possibile richiamare i metodi dei servizi Web, ad esempio per la visualizzazione o per la creazione delle richieste, poiché è negato l'accesso al gruppo funzioni di Call Manager.

Quando l'applicazione completa le attività per un determinato utente, richiamare il metodo Logout() per invalidare il SID.

Dopo un determinato periodo di inattività, i SID scadono. Ovvero, un SID scade se l'intervallo tra le chiamate dei metodi è maggiore del valore di timeout specificato. L'intervallo di timeout viene impostato in Gestione opzioni ed è specificato dall'opzione CA Service Desk Manager seguente:

`'webservice_session_timeout'`

Se questo valore viene impostato su zero (0), il SID non scade mai. Se manca questa opzione oppure se non è impostata, il valore predefinito è 1 ora. Se viene richiamato un metodo di un servizio Web con un SID scaduto, la prima volta a cui viene fatto riferimento a esso viene restituito un errore con il codice UDS_SESSION_TIMEOUT e con il codice UDS_BAD_SESSION le volte successive.

Per mantenere attivo un SID, richiamare i metodi dei servizi Web prima del raggiungimento del timeout. Per mantenere attivo il SID senza utilizzare il server, richiamare il metodo serverStatus().

Opzione Servizio Web

È possibile indirizzare il traffico a un domsrvr diverso dal domsrvr primario per una sessione di un servizio Web. Accedere a queste opzioni da Gestione opzioni, Servizio Web. Le opzioni seguenti controllano la sessione del servizio Web:

webservice_session_timeout

Consente di impostare il valore di timeout (in minuti) per le sessioni dei servizi Web. Se la durata tra le chiamate successive ai metodi Web è superiore rispetto al valore specificato qui, l'ID sessione viene contrassegnato come scaduto e non sarà più valido.

Per evitare che le sessioni scadano a causa dell'attività, impostare il valore di questa opzione su 0. Le sessioni potrebbero essere invalidate dagli altri metodi, ad esempio le routine di disconnessione.

webservice_domsrvr

Consente di specificare il nome del motore oggetti che utilizzano i servizi Web. Se non è installato, verrà utilizzato "domsrvr".

Il valore di questa opzione deve essere una stringa che inizia con i caratteri "domsrvr:".

Nota: queste opzioni richiedono il riavvio del server di CA Service Desk Manager e Windows IIS Service.

Gestione e controllo dell'accesso

Per ridurre al minimo il potenziale problema del flooding dei ticket dei servizi Web e per mantenere la stabilità del server di CA Service Desk Manager, questa versione dei servizi Web di CA Service Desk Manager utilizza un sistema di gestione e controllo dell'accesso. Lo scopo principale di questo sistema è gestire l'eccessiva attività del servizio da parte delle applicazioni utente causata da errori di programmazione o da eccezioni. Rappresenta inoltre un metodo per impedire l'accesso ai servizi Web CA Service Desk Manager a eventuali utenti malintenzionati. Un amministratore di un'applicazione di un servizio Web può creare e definire una norma di accesso in CA Service Desk Manager per controllare l'accesso ai servizi Web di CA Service Desk Manager da un'applicazione del servizio Web.

Nota: viene fornita una norma di accesso predefinita con codice DEFAULT. La norma di accesso predefinita non contiene limitazioni di accesso e viene applicato solo alle sessioni autenticate tramite il nome utente e la password.

Definizione di una norma di accesso

Per creare qualsiasi norma di accesso per i servizi Web, un amministratore deve definire una norma di accesso.

Per definire la norma di accesso

1. Fare clic sulla scheda Amministrazione.
2. Nella struttura a sinistra fare clic su Web Services Policy, Policies.

Viene visualizzato l'elenco di norme di accesso ai servizi Web.

3. Fare clic su Crea nuovo.

Viene visualizzata la pagina Crea Nuova norma di accesso servizi Web.

4. Immettere le informazioni per la nuova norma di accesso.

Nota: il valore predefinito -1 in qualsiasi contatore di operazioni indica che non sono presenti limitazioni per l'operazione corrispondente. Un valore 0 (zero) indica che l'operazione corrispondente non è consentita.

Simbolo

(Obbligatorio) Identifica il nome simbolico della norma di accesso.

Codice

(Obbligatorio) Indica il testo univoco che identifica questa norma di accesso.

Stato

(Richiesto) Identifica lo stato di un criterio di accesso. Una norma inattiva non viene utilizzata.

Contatto Proxy

Identifica il contatto da utilizzare per tutte le operazioni dei servizi Web e per la protezione di CA Service Desk Manager.

Predefinito

Identifica la norma predefinita. Impostare questo criterio come predefinito. È consentita la presenza di un solo criterio predefinito attivo. La creazione di una nuova norma predefinita imposta automaticamente la norma predefinita corrente su uno stato non predefinito.

Con chiave

(Sola lettura) Indica se una chiave pubblica è stata associata a questa norma. Questo campo viene aggiornato quando una chiave pubblica viene associata a un criterio tramite l'utilità pdm_pki.

Consenti rappresentazione

Identifica il privilegio allow impersonate. se questo campo è impostato, il segnaposto può richiamare il metodo di servizi Web impersonate() e creare una nuova sessione di servizi Web a nome dell'utente rappresentato. Quando si crea la nuova sessione non viene eseguita un'ulteriore autenticazione per l'accesso. Tuttavia, questo metodo può essere richiamato con successo solo quando il valore di access_level del tipo di accesso del nuovo utente è inferiore o uguale al valore di grant_level del tipo di accesso dell'utente proxy.

Descrizione

Riporta la descrizione dettagliata di questo criterio di accesso.

Creazione ticket

Indica il numero di operazioni di inserimento di ticket (richiesta di chiamata, ordine di cambiamento e questione) consentito ogni ora.

Creazione oggetto

Indica il numero di operazioni di inserimento di oggetti di CA Service Desk Manager (diversi dall'oggetto ticket) consentito ogni ora.

Aggiornamenti oggetto

Indica il numero di operazioni di aggiornamento degli oggetti di CA Service Desk Manager consentito ogni ora.

Allegati

Indica il numero di operazioni di associazione consentito ogni ora.

Query dati

Indica il numero di operazioni di query sui dati consentito ogni ora.

Conoscenza

Indica il numero di operazioni della conoscenza consentito ogni ora.

5. Fare clic su Salva.

Metodi dei servizi Web per categoria

Ogni metodo dei servizi Web di CA Service Desk Manager appartiene a una categoria specifica. Di seguito sono riportate le categorie e i metodi corrispondenti:

Creazione ticket

- createTicket()
- createQuickTicket()

- createRequest()
- createChangeOrder()
- createIssue()

Creazione oggetto

- logComment()
- createAsset()
- addAssetLog()
- createAssetParentChildRelationship()
- createObject()
- createWorkFlowTask()
- createActivityLog()
- notifyContacts()
- addBookmark()
- addComment()
- createFolder()

Aggiornamenti oggetto

- addMemberToGroup()
- removeMemberFromGroup()
- closeTicket()
- createLrelRelationships()
- removeLrelRelationships()
- deleteWorkFlowTask()
- updateObject()
- transfer()
- escalate()
- attachChangeToRequest()
- detachChangeFromRequest()
- changeStatus()
- clearNotification()
- updateLrel()
- deleteBookmark()
- updateRating()

Allegati

- createAttmnt()
- createAttachment()
- attachURLLink()
- deleteAttmnt()
- deleteComment()
- removeAttachment()

Query dati

- impersonate()
- serverStatus()
- getBopsid()
- getConfigurationMode()
- getHandleForUserid()
- getAccessTypeForContact()
- getPermissionsGroup
- getObjectTypeInformation()
- getRelatedList()
- getRelatedListValues()
- getGroupMemberListValues()
- getPendingChangeTasksForContact()
- getPendingIssueTasksForContact()
- getWorkFlowTemplates()
- getWorkflowTemplateList()
- getTasksListValues()
- getNotificationsForContact()
- getPolicyInfo()
- getAssetExtensionInformation()
- getLrelValues()
- getObjectValues()
- doSelect()
- doQuery()
- getPropertyInfoForCategory()

- `getValidTaskTransitions()`
- `getListValues()`
- `getListInfo()`
- `findContact()`
- `getAttmntInfo()`
- `getAttmntList()`
- `getBookmarks()`
- `getCategory()`
- `getComments()`
- `getContact()`
- `getDecisionTrees()`
- `getDocument()`
- `getDocumentTypes()`
- `getFolderInfo()`
- `getFolderList()`
- `getLrelLength()`
- `getPriorities()`
- `getRepositoryInfo()`
- `getStatuses()`
- `getTemplateList()`

Conoscenza

- `createDocument()`
- `deleteDocument()`
- `doSelectKD()`
- `faq()`
- `attmntFolderLinkCount()`
- `getAttmntListPerKD()`
- `isAttmntLinkedKD()`
- `getDocumentByIDs()`
- `getKDListPerAttmnt()`
- `getQuestionsAsked()`

- `modifyDocument()`
- `rateDocument()`
- `search()`

Quando CA Service Desk Manager aggiorna un criterio di accesso, i servizi Web aggiornano dinamicamente le informazioni corrispondenti al criterio. Le sessioni dei servizi Web attive controllate da questo criterio rimangono controllate con le configurazioni del criterio. Per gestire e controllare questo criterio, le nuove sessioni dei servizi Web utilizzano le configurazioni più aggiornate.

Nota: per informazioni su ciascun metodo, vedere la *Guida di riferimento tecnico di CA Service Desk Manager*.

Definizione di un tipo di errore

I *tipi di errore* vengono assegnati durante la creazione dei ticket e un criterio di accesso ne definisce un set. Un'applicazione utente dei servizi Web di CA Service Desk Manager può utilizzare metodi Web di basso livello per creare un ticket (richiesta, ordine di cambiamento o questione) specificando uno di questi tipi per classificare l'errore indicato nel ticket. I tipi di errore possono essere utilizzati solo con il metodo di alto livello `createTicket()`. I metodi di basso livello, ad esempio `createRequest()`, non utilizzano tipi di errore.

Ulteriori informazioni:

[Accesso semplificato ai servizi Web](#) (a pagina 506)

Tipi di errore dei servizi Web

I servizi Web di CA Service Desk Manager includono inoltre un set definito di tipi di errore predefiniti creati per *ogni* criterio. Questi tipi predefiniti, specificati come tipi di errore *interni*, possono essere disattivati ma mai eliminati. Nel prodotto è possibile utilizzare la pagina Dettagli criterio di accesso servizi Web per visualizzare i tipi di errore predefiniti visualizzati quando viene creato un nuovo criterio.

Di seguito viene descritto ogni tipo di errore interno:

ACCESS_ERROR

Indica che il sistema non riesce a collegarsi a una risorsa oppure a individuarla, ad esempio un file, un sito Web e così via.

EXCEPTION_FATAL

Indica l'arresto imprevisto dell'applicazione.

EXCEPTION_RUNTIME

Indica che il codice dell'applicazione ha rilevato un'eccezione.

LOGIN_ERROR

Indica che l'operatore non riesce ad accedere all'applicazione.

Atri tipi di errore

L'amministratore di un criterio di accesso può aggiungere altri tipi di errore come descritto nelle informazioni seguenti:

Tipo di errore	Descrizione
Modello ticket	Identifica un modello per un incidente, errore, questione oppure ordine di cambiamento utilizzato per creare un ticket quando viene segnalato questo tipo di errore. Nota: il contatto proprietario del criterio viene utilizzato come utente finale. Tipo ticket e Nome modello ticket definiscono il modello di ticket.
Predefinito	Indica se questo tipo di errore è il tipo predefinito per il criterio. Per ogni criterio è concesso un solo problema predefinito. Nota: l'impostazione di un nuovo tipo di errore predefinito sovrascrive quello esistente associato al criterio.
Attivo	Rappresenta un tipo di errore attivo. Nota: un tipo non attivo non crea ticket.
Interna	Identifica il campo come di sola lettura, per indicare se si tratta di un tipo di errore interno predefinito.
Simbolo	Indica il nome simbolico del tipo di errore.
Codice	Indica l'identificativo di testo univoco del tipo di errore.
Descrizione	Specifica la descrizione dettagliata del tipo di errore.
Gestione duplicati	Definisce l'azione da intraprendere quando il prodotto rileva la presenza di un ticket identico.
Dati restituzione	Identifica il messaggio di restituzione per le applicazioni client definito dall'utente che è possibile specificare per il metodo Web

Tipo di errore	Descrizione
	"createTicket()". Il tipo di problema Dati restituzione può essere utilizzato per indicare un'azione che l'applicazione deve eseguire (Restituzione dati applicazione) oppure un messaggio (Restituzione dati utente) da visualizzare all'utente finale.

Ulteriori informazioni:

[Gestione dei ticket duplicati](#) (a pagina 505)

Gestione dei ticket duplicati

La norma di accesso del servizio Web può rilevare e gestire i ticket duplicati. Questa norma è utile per evitare il flooding dei ticket. Un ticket creato con la capacità di essere un duplicato è valido se sono soddisfatte tutte le condizioni seguenti:

- È presente almeno un altro ticket dello stesso tipo (cr, iss o chg) ATTIVO.
- Il ticket esistente è stato creato dal servizio Web.
- Il ticket esistente è stato creato con la stessa norma e tipo di errore del ticket che si sta creando.
- Il valore del campo "data creazione" del ticket esistente si trova all'interno di un limite specificato, ad esempio, il ticket è stato aperto meno di due giorni fa.

Nota: il campo della data di creazione viene configurato utilizzando il valore presente in Intervallo di tempo massimo per la ricerca dei duplicati.

- L'ID duplicato corrisponde a un ID che gli utenti hanno specificato quando hanno richiamato il metodo createTicket().

Anche gli utenti possono contribuire ad evitare la creazione dei duplicati classificando i ticket come univoci o differenti, in base ai criteri noti all'utente. A tale scopo, aggiungere un parametro opzionale di tipo stringa alla chiamata ai servizi Web createTicket. Se la gestione dei duplicati è attiva, il parametro string viene verificato dopo aver controllato la corrispondenza degli altri criteri di gestione dei duplicati per determinare se si tratta di una chiamata univoca o duplicata a questo metodo.

Duplicazione dei risultati del ticket

Se l'azione di creazione del ticket genera un duplicato, il tipo di errore esistente può essere configurato per eseguire una delle operazioni seguenti:

Tipo di errore riconfigurato	Risultati
Creare il nuovo ticket e ignorare i duplicati	Vengono restituiti un nuovo handle e un nuovo numero di ticket (predefinito).
Non creare un nuovo ticket; aggiungere invece un registro attività al duplicato esistente	Vengono restituiti l'handle di ticket e il numero di ticket esistente.
Non creare un nuovo ticket; aggiungere una voce al registro standard CA Service Desk Manager	Vengono restituiti un handle di ticket e il numero di ticket esistente.
Creare un nuovo ticket e associarlo come figlio al duplicato	Vengono restituiti un nuovo handle e un nuovo numero di ticket.

Accesso semplificato ai servizi Web

I servizi Web di CA Service Desk Manager forniscono un set ridotto di metodi dei servizi Web di alto livello che rappresentano versioni semplificate dei metodi dei servizi Web esistenti. Per la maggior parte delle applicazioni degli utenti l'utilizzo di un set esteso di metodi dei servizi Web non è indispensabile per poter richiedere i servizi di Service Desk tramite i servizi Web di CA Service Desk Manager. Lavorando a stretto contatto con le norme di accesso definiti dall'utente e utilizzando i parametri predefiniti specificati nelle norme, questo set di metodi generali dei servizi Web può essere utilizzato con una minima conoscenza dello schema oggetti di CA Service Desk Manager. I metodi di alto livello includono inoltre un set comune di funzionalità CA Service Desk Manager necessarie per la maggior parte delle applicazioni per il riconoscimento dei servizi.

Di seguito viene descritto l'utilizzo dei metodi generali dei servizi Web:

createTicket (SID, Description, Error_Type, Userid, Asset, DuplicationID)

Se si utilizza questo metodo è necessario specificare un tipo di errore per l'errore segnalato. Il tipo di errore deve contenere il modello di ticket appropriato per il ticket da creare. Deve definire l'azione da eseguire in caso di ticket duplicato, specificare gli output dei dati e infine deve essere associato alla norma di accesso definito per l'applicazione dell'utente.

Quando viene richiamato questo metodo, i servizi Web di CA Service Desk Manager individuano il tipo di errore e la norma di accesso corrente necessari per la creazione del ticket. Di seguito viene mostrata la sequenza che i servizi Web di CA Service Desk Manager utilizzano per individuare il tipo di errore appropriato:

- Se come input viene fornito il codice di un tipo di errore specifico che corrisponde a un tipo di errore associato al criterio, viene utilizzato questo tipo di errore, indipendentemente dal fatto che sia o meno interno.
- Se non viene specificato alcun tipo di errore oppure durante il passaggio precedente non viene individuato un tipo di errore, viene utilizzato il tipo di errore predefinito se per il criterio ne è definito uno.
- Se per il criterio non esiste un tipo di errore predefinito oppure il passaggio precedente non riesce, viene utilizzato il tipo di errore predefinito specificato per i tipi di errore interni.

Dopo aver definito un tipo di errore, i servizi Web di CA Service Desk Manager lo utilizzano per creare un ticket. L'utente proxy definito nella norma di accesso viene utilizzato per la creazione del ticket se l'ID utente è vuoto e le informazioni sull'asset vengono aggiunte al ticket (se il valore di input non è vuoto). Dopo la creazione del ticket, i servizi Web di CA Service Desk Manager restituiscono i dati dell'utente e dell'applicazione, come specificato dal tipo di errore.

closeTicket (SID, Description, TicketHandle)

Gli utenti possono richiamare questa funzione per chiudere un ticket aperto. Imposta semplicemente lo stato di un ticket aperto su 'chiuso' e aggiunge la descrizione dell'input al registro attività.

logComment(SID, TicketHandle, Comment, Internal_Flag)

Aggiunge una voce con il commento dell'input al registro attività del ticket aperto.

getPolicyInfo(SID)

Consente agli utenti di ottenere le informazioni sulla norma che controllano la sessione corrente dei servizi Web. È possibile utilizzare queste informazioni come un indicatore della capacità del server per questa applicazione dell'utente. Gli utenti possono adattare le proprie chiamate ai servizi Web in base alla capacità del server.

Questo set di API semplificate per i servizi Web riduce sensibilmente lo sforzo richiesto alla maggior parte degli utenti per comprendere il set completo di API per i servizi Web e lo schema di CA Service Desk Manager. Il loro utilizzo semplifica e accelera il processo di creazione di applicazioni abilitate al riconoscimento dei servizi.

Oggetti

CA Service Desk Manager considera ogni entità, ad esempio un contatto o una questione, come un *oggetto*. Questi oggetti di alto livello sono definiti nei file majic (.maj) e mod (.mod) sul server CA Service Desk Manager nella directory seguente:

```
/bopcfg/majic
```

Gli oggetti personalizzati sono definiti nella directory seguente:

```
/site/mods/majic
```

Gli oggetti sono essenzialmente wrapper generali disponibili in una tabella di database.

Un tipo di oggetto (talvolta chiamato *factory*) definisce l'oggetto. Ad esempio, gli oggetti Richiesta appartengono al tipo 'cr'. Ogni tipo di oggetto viene definito dalla dichiarazione "OBJECT" in un file majic.

Nota: tutti gli oggetti forniti con CA Service Desk Manager vengono enumerati nella Guida di riferimento tecnico di CA Service Desk Manager.

Un oggetto dispone di *attributi*, che sono essenzialmente colonne di una tabella di database (da non confondersi con gli attributi XML). I servizi Web offrono molti metodi per recuperare i valori degli attributi. Molti metodi richiedono l'assegnazione dei nomi agli attributi per impostare o recuperare i valori. È necessario utilizzare il nome di attributo assegnato nel file majic o mod che definisce l'oggetto, che può essere differente dal nome di database effettivo. I siti client possono aggiungere altri attributi come personalizzazione.

Nota: per un elenco completo di tutti gli attributi per ogni oggetto, consultare la *Guida di riferimento tecnico di CA Service Desk Manager*.

I servizi Web identificano in modo univoco un oggetto dal relativo *handle*, ovvero un valore di tipo stringa in formato *objectType:ID*, dove *objectType* è il nome del tipo (factory) di oggetto e ID è un valore univoco. Il valore ID corrisponde a quello dell'attributo 'id' presente in qualsiasi oggetto di CA Service Desk Manager. Poiché l'attributo 'id' è quasi sempre indicizzato nel DBMS, l'utilizzo della parte id dell'handle dell'oggetto è particolarmente importante per creare query efficienti. Ogni oggetto, indipendentemente dal tipo, memorizza questo valore in un attributo dell'oggetto denominato "persistent_id".

Nota: nelle versioni precedenti la parte ID dell'handle è sempre costituita da una stringa di valori interi. In Unicenter Service Desk r11.0 e versioni successive la parte ID può anche essere la rappresentazione stringa di un UUID, in genere di 32 caratteri.

Nella tabella seguente sono elencati i nomi di oggetto e factory delle entità che utilizzano gli UUID:

Nome oggetto	Nome factory
Contatto	cnt
Asset	nr
Organization	org
Ubicazione	loc
Società/Fornitore	ca_cmpny
Modello	mfrmod

Gli handle sono *persistenti*; un handle che rappresenta un oggetto specifico è sempre univoco per tutta la sua durata, anche nelle migrazioni del database. I client possono avvalersi di questa persistenza quando utilizzano gli oggetti statici, ad esempio gli oggetti Stato o Tipi contatto.

Gli handle degli oggetti sono essenziali per utilizzare correttamente i servizi Web di CA Service Desk Manager. Molti metodi, specialmente quelli che aggiornano i dati, richiedono l'utilizzo degli handle. La maggior parte dei metodi che restituisce i dati dell'oggetto include anche l'handle dell'oggetto.

Aggiornamenti del sistema (cache)

I servizi Web memorizzano nella cache informazioni per i tipi di oggetto. Queste informazioni non vengono inserite nella cache finché non viene fatto riferimento al tipo per la prima volta con conseguente leggero ritardo nell'elaborazione.

Per evitare ritardi al server o alle operazioni della cache, è possibile eseguire client preliminare per attivare i servizi Web e inserire nella cache le informazioni sul tipo di oggetto più comune. Il modo più semplice per inserire nella cache le informazioni sul tipo di oggetto è eseguire chiamate ripetute al metodo `GetObjectTypeInfo()`. Il tipo di oggetto da prendere in considerazione per questa tecnica può essere uno di quelli riportati di seguito:

Tipo oggetto	Definizione
cr	Filtro
chg	Ordine di cambiamento
iss	Questione
cnt	Contatto

Tipo oggetto	Definizione
nr	Asset
wf	CA Workflow (Ordini di cambiamento)
iss_wf	CA Workflow (questioni)
prp	Proprietà (per cambiamento e questione)
prptpl	Modello proprietà (per cambiamento e questione)
cr_prp	Proprietà richiesta
cr_prptpl	Modello proprietà richiesta

Aggiungere qualsiasi tipo di oggetto aggiuntivo a cui fa riferimento il proprio codice client.

Categorie e proprietà

Gli oggetti di tipo Richiesta, Ordine di cambiamento e Questione dispongono tutti di un campo Categoria, che viene utilizzato per classificare la natura del ticket. Per una categoria è possibile che siano presenti oggetti proprietà, che vengono associati al ticket al momento dell'assegnazione della categoria. Alcuni di questi oggetti possono essere contrassegnati come *obbligatori*, il che significa che è necessario specificare un valore per poter salvare il ticket. Questo è valido sia per le operazioni di inserimento che di aggiornamento.

I servizi Web di CA Service Desk Manager forniscono automaticamente valori predefiniti per tutti i ticket creati con i servizi Web. Il valore predefinito, al momento "-", è ricavato dal catalogo dei messaggi localizzati di CA Service Desk Manager.

Per impostare i valori delle proprietà al momento della creazione, sono disponibili tre metodi di creazione dei ticket: `createChangeOrder`, `createIssue` e `createRequest`. Ognuno di questi metodi dispone di un parametro che consente il passaggio dei valori per qualsiasi proprietà. Per scoprire le proprietà che verranno associate, è necessario individuare le proprietà associate alla categoria da assegnare al ticket. Il metodo più semplice da utilizzare è `getPropertyInfoForCategory()`.

Nota: per ulteriori informazioni su `getPropertyInfoForCategory()`, consultare la *Guida di riferimento tecnico di CA Service Desk Manager*.

Per identificare i valori validi per una proprietà, individuare innanzitutto la regola di validazione proprietà per il modello di proprietà appropriato. A tale scopo, richiedere l'attributo `validation_rule` durante la chiamata al metodo `getPropertyInfoForCategory`. Recuperare quindi il `validation_type` associato alla regola. Se il tipo è dropdown, è quindi possibile utilizzare il metodo `getRelatedList` per recuperare i valori associati alla regola, utilizzando l'attributo BREL "values" nell'oggetto `prpval_rule`.

Nota: per ulteriori informazioni, consultare la *Guida di riferimento tecnico di CA Service Desk Manager*.

Per impostare i valori delle proprietà dopo un'operazione di aggiornamento con il metodo `updateObject()`, è necessario interrogare l'elenco delle proprietà dopo l'aggiornamento. Per eseguire questa attività può essere utile il metodo `getRelatedList()`.

La validazione dei valori delle proprietà mediante i metodi dei servizi Web al momento non è supportata. Per assegnare, ad esempio, valori di proprietà a una regola di validazione con un tipo di validazione per l'opzione elenco a discesa, è necessario scrivere codice aggiuntivo per creare valori di proprietà durante la creazione della regola di validazione per l'opzione elenco a discesa. Non collegare un valore di proprietà a una regola di validazione per la casella di controllo.

Nota: per ulteriori informazioni sulle regole di validazione per le proprietà, consultare la *Guida all'amministrazione*. Per informazioni sulla creazione di regole di validazione per le proprietà mediante l'interfaccia di CA Service Desk Manager, vedere la *Guida in linea*.

Restituzione degli oggetti in formato XML

Molti dei metodi dei servizi Web restituiscono una rappresentazione XML degli oggetti di CA Service Desk Manager. I servizi Web utilizzano una struttura XML standard che inizia con l'elemento principale seguente:

```
<UDSObject>
```

Il formato della rappresentazione XML viene descritto nella tabella seguente:

Elemento XML	Tipo	Descrizione
<UDSObject>	N/D	Identifica il nodo principale.
<Handle>	Stringa	Identifica l'handle dell'oggetto.

Elemento XML	Tipo	Descrizione
<Attributes>	Sequenza	Identifica i valori di attributo. Contiene zero o più elementi per i valori di attributo dell'oggetto.
<attrName0 DataType = "typeEnum">	Stringa	Identifica <i>AttrName0</i>, che è un nome di attributo dell'oggetto, come definito nel file majic (.maj) o mod (.mod) di CA Service Desk Manager. Questo nome può utilizzare la notazione a punti, in base al metodo Web utilizzato. Il valore dell'elemento è il valore dell'attributo. Un elemento vuoto indica un valore Null/vuoto per questo attributo dell'oggetto. L'attributo DataType è un valore intero che indica il tipo di dati dell'attributo nell'ambiente di CA Service Desk Manager. Nota: per informazioni sul valore dell'attributo DataType, consultare la <i>Guida di riferimento tecnico</i>.

Ad esempio, una chiamata al metodo `getObjectValues()` può restituire le informazioni riportate di seguito:

```
<UDSObject>
  <Handle>cnt:555A043EDDB36D4F97524F2496B35E75</Handle>
  <Attributes>
    <Attribute DataType="2003">
      <AttrName>first_name</AttrName>
      <AttrValue>first name</AttrValue>
      <DisplayValue>Yaakov</DisplayValue>
    </Attribute>
    <Attribute DataType="2005">
      <AttrName>organization</AttrName>
      <AttrValue>342</AttrValue>
      <DisplayValue>Accounting Crew</DisplayValue>
    </Attribute>
  </Attributes>
  <Lists>
    <List name="mylist1">
      <UDSObject>...</UDSObject>
      <UDSObject>...</UDSObject>
    </List>
  </Lists>
</UDSObject>
```

Alcuni metodi, ad esempio `doSelect()`, restituiscono una sequenza di elementi `<UDSObject>` contenuti in un elemento `<UDSObjectList>`.

La sezione `<Lists>` contiene zero o più nodi `<List>`. Un nodo `<List>` contiene zero o più nodi `<UDSObject>`. Gli elementi `<List>` vengono generalmente restituiti solo quando viene creata una richiesta specifica di valori elenco.

Quando si desidera restituire un elenco di valori relativi a un oggetto specifico, è necessario utilizzare il metodo `getRelatedListValues`.

Nota: per informazioni sul metodo `getRelatedListValues`, consultare la *Guida di riferimento tecnico*.

Se viene eseguita una richiesta per un solo elenco senza il nome dell'attributo, ad esempio `actlog`, nella sezione `<List>` viene restituito l'intero elemento `<UDSObject>`.

Naturalmente, i metodi specifici, ad esempio `getDocument()`, possono essere differenti. Quando viene effettuata una richiesta per un attributo, viene restituito il valore del database. Per gli attributi SREL, questo potrebbe non essere molto utile. Quando si richiede l'attributo assignee di un oggetto Richiesta, viene restituito un valore intero poiché l'attributo REL_ATTR dell'oggetto Contatto (chiave esterna) rappresenta il relativo ID. In Unicenter Service Desk r11.0 i dati di restituzione per gli attributi includono elementi per il DBMS e il valore di nome comune dei riferimenti SREL.

Nota: per informazioni sull'impostazione di attributi SREL con valori chiave esterna, consultare la *Guida di riferimento tecnico*.

ITIL, metodologia

Per impostazione predefinita, i servizi Web offrono un supporto completo per la metodologia ITIL. Le funzionalità ITIL di CA Service Desk Manager consentono di usufruire di tale metodologia.

Creazione di incidenti o problemi

CA Service Desk Manager supporta la metodologia ITIL in modo da consentire la creazione di incidenti e problemi mediante i servizi Web di CA Service Desk Manager. Gli incidenti e i problemi sono contenuti nell'oggetto `cr` (`Call_Req`). Il relativo attributo `type` distingue il record come incidente, problema o richiesta. Per creare una richiesta, un incidente o un problema, chiamare il metodo `createRequest` e specificare il valore appropriato per l'attributo `type`.

L'attributo `type` è un puntatore (SREL) all'oggetto `crt` (`Call_Req_Type`), è quindi necessario passare un handle come valore.

Gli esempi di codice seguenti illustrano come creare un incidente o problema passando l'handle `crt` corretto al metodo `createRequest`. L'impostazione dell'attributo `type` nella coppia nome-valore che viene passata come parametro al metodo `createRequest` crea i ticket:

Esempio: sintassi per un problema

```
attrVals = {"riepilogo", "Un nuovo problema", "descrizione", "nuovo problema", "tipo", "crt:181"}
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new String[0])
```

Esempio: sintassi per un incidente

```
attrVals = {"riepilogo", "Un nuovo incidente", "descrizione", "nuovo incidente", "tipo", "crt:182"}
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new String[0])
```

Ulteriori informazioni:

[Handle predefiniti](#) (a pagina 517)

Query per incidenti o problemi

Per recuperare gli incidenti o i problemi, includere l'attributo *type* dell'oggetto *cr* nella clausola *where*. L'esempio seguente mostra una clausola *where* per il recupero di tutti gli incidenti attivi. La clausola *where* può essere utilizzata con i metodi che eseguono le query per gli oggetti '*cr*', ad esempio *doSelect* e *doQuery*:

```
type.id = 182 AND active = 1
```

Il valore "182" è la parte ID dell'*handle* che rappresenta i tipi di incidente.

Nota: per ulteriori informazioni, vedere la tabella di oggetti *crt* (*Call_Req_Type*) illustrata in [Handle predefiniti](#) (a pagina 517). Per ulteriori informazioni sulla creazione di query corrette, vedere [Clausola WHERE](#) (a pagina 270).

Associazione di un incidente a un problema

I servizi Web possono creare associazioni tra ticket ITIL, ad esempio l'associazione di uno o più incidenti a un problema. L'attributo padre di un ticket viene utilizzato per creare relazioni di tipo padre-figlio tra gli oggetti *cr*, utilizzati per gli oggetti di tipo Richiesta, Incidente e Problema. L'impostazione dell'attributo padre di un ticket per puntare a un altro ticket crea la relazione.

Ad esempio, un incidente appena creato fa riferimento a un problema esistente. Per associare l'incidente al problema e impostare l'attributo padre dell'incidente, utilizzare *UpdateObject*. L'esempio di codice seguente mostra quanto detto impostando l'attributo padre sull'*handle* di un ticket di problema esistente:

```
attributeValues = {"padre", "cr:12346"}  
USPSD.UpdateObject(SID, incidentHandle, attributeValues, new String [0])
```

Associazione di un problema a un ordine di cambiamento

Gli incidenti e i problemi possono essere collegati agli ordini di cambiamento utilizzando il metodo `attachChangeToRequest`. Nell'esempio di codice seguente viene utilizzato questo metodo per creare un ordine di cambiamento e associarlo contemporaneamente a un problema. Nell'esempio "cr:12347" è l'handle di oggetto del problema. Passa un handle vuoto per il quarto parametro, permettendo al metodo di creare un ordine di cambiamento:

```
UPSPSD.attachChangeToRequest(SID, creatorHandle, "cr:12347", "", new String[0], "activity description")
```

Elementi di configurazione

La metodologia ITIL utilizza il termine *elemento di configurazione* per fare riferimento al software, all'hardware e ad altre risorse IT. Questo termine si riferisce all'oggetto "nr" archiviato nella tabella di database delle risorse CA. Anche tutti i metodi basati sugli oggetti *asset* utilizzano gli elementi di configurazione. L'unica differenza è nella terminologia.

Utilizzo dei servizi Web

Le informazioni contenute in questa sezione forniscono i concetti di base per l'utilizzo dei servizi Web di CA Service Desk Manager. Nella directory di installazione di CA Service Desk Manager che segue è presente un codice di esempio che utilizza i servizi Web:

```
<NX_ROOT>/samples/sdk/websvc/java
```

Il codice di esempio è scritto in Java utilizzando Apache Axis per la messaggistica SOAP.

Accessi

Per poter utilizzare un metodo per i servizi Web, è necessario ottenere un SID (ID sessione) da uno dei metodi seguenti: `login()`, `loginService()` e `loginServiceManaged()`. I primi due metodi richiedono l'utilizzo di un nome utente e di una password che vengono convalidati esattamente come avviene per l'interfaccia Web di CA Service Desk Manager. L'oggetto Tipo di accesso del contatto specifica il metodo di validazione. Il terzo metodo richiede una coppia di chiavi pubblica/privata, in cui la richiesta di accesso crittografata con la chiave privata può essere decifrata solo con la chiave pubblica e viceversa.

Ulteriori informazioni:

[Specifiche esterne](#) (a pagina 487)

Modalità di esecuzione di attività comuni

I servizi Web rappresentano un'API flessibile e potente in CA Service Desk Manager ma richiedono una conoscenza della struttura a oggetti utilizzata dal prodotto. A tale scopo:

1. Familiarizzare con le informazioni su oggetti e attributi contenute nella *Guida di riferimento tecnico di CA Service Desk Manager*. In questa guida sono elencati gli attributi di ciascun oggetto del sistema, che sono essenziali poiché molti metodi dei servizi Web richiedono l'utilizzo dei nomi degli attributi.
2. Esaminare i metodi dei servizi Web, soprattutto quelli generici. Se, ad esempio, l'applicazione deve visualizzare tutti i registri attività per una richiesta, identificare innanzitutto in che modo i registri sono correlati alla richiesta. Secondo la *Guida di riferimento tecnico di CA Service Desk Manager* l'oggetto Richiesta dispone di due elenchi di registri attività: l'elenco act_log (che mostra solo registri non interni) e l'elenco act_log_all (che elenca tutti i registri attività).
3. Identificare i metodi dei servizi Web necessari. Per associare gli elenchi a un oggetto, utilizzare i metodi getRelatedList() o getRelatedListValues().

Handle predefiniti

Alcuni dati predefiniti forniti dal prodotto vengono utilizzati di frequente. Per non dover cercare gli handle per tali oggetti, quelli più utilizzati sono elencati nelle tabelle seguenti.

Nota: diversamente dagli handle che non possono essere modificati, è possibile modificare i simboli leggibili.

Tipo contatto (Nome oggetto: ctp)

Handle	Nota
ctp:2307	Il tipo di "Analista"
ctp:2310	Il tipo di "Cliente"
ctp:2305	Il tipo di "Dipendente"
ctp:2308	Il tipo di "Gruppo"

Impatto (Nome oggetto: imp)

Handle	Nota
imp:1605	Impatto 'Nessuno'
imp:1600	Impatto basso '5'

Handle	Nota
imp:1601	Impatto medio-alto '4'
imp:1602	Impatto medio '3'
imp:1603	Impatto medio-alto '2'
imp:1604	Impatto alto '1'

Priorità (Nome oggetto: pri)

Handle	Nota
pri:505	Priorità non assegnata 'Nessuna'
pri:500	Priorità bassa '5'
pri:501	Priorità medio-bassa '4'
pri:502	Priorità media '3'
pri:503	Priorità medio-alta '2'
pri:504	Priorità alta '1'

Gravità (Nome oggetto: sev)

Handle	Nota
sev:800	Gravità bassa '1'
sev:801	Gravità medio-alta '2'
sev:802	Gravità media '3'
sev:803	Gravità medio-alta '4'
sev:804	Gravità alta '5'

Tipo richiesta chiamata (Nome oggetto: crt)

Handle	Nota
crt:180	Filtro
crt:181	Problema
crt:182	Incident

Query per gli oggetti Richiesta, Questioni o Ordini di cambiamento assegnati a un oggetto Contatto

Una delle operazioni più comuni è il recupero delle richieste attive assegnate a un analista (assegnatario). È possibile utilizzare uno dei metodi disponibili, ad esempio `doQuery()` (per ottenere un riferimento all'elenco) oppure `doSelect()` (per ottenere immediatamente i valori). Supponendo che l'handle dell'assegnatario sia già noto, la clausola `where` da utilizzare è la seguente:

```
assignee.id = U'<assigneeID>' AND active = 1
```

In questa clausola `Where`, `<assigneeID>` è la parte id dell'handle di un contatto, un valore quale, "555A043EDDB36D4F97524F2496B35E75".

Questa clausola `where` è valida per le richieste, gli ordini di cambiamento e le questioni poiché dispongono tutti degli attributi 'assignee' e 'active' che hanno lo stesso significato per tutti e tre i tipi di oggetti. La parte `'active = 1'` della clausola `where` limita la ricerca alle richieste attive.

Il flag attivo

La maggior parte degli oggetti di CA Service Desk Manager dispone di un campo chiamato 'active' o 'delete_flag'. Si tratta di un puntatore SREL all'oggetto `Active_Boolean_Table` o all'oggetto `Boolean_Table`. Prendere in considerazione l'aggiunta di questi campi alle proprie query per filtrare gli oggetti contrassegnati come non attivi dall'amministratore del sistema. Per l'esecuzione delle query, ricercare `'delete_flag = 0'` per trovare i record attivi e `'delete_flag = 1'` per trovare quelli non attivi. Ad esempio, lo pseudo-codice seguente dimostra l'utilizzo del metodo `doSelect()` per recuperare i valori per tutti gli oggetti attivi Stato richiesta:

```
doSelect(SID, "crs", "delete_flag = 0", -1, new String[0]);
```

Per impostare un oggetto sullo stato attivo o non attivo, è necessario passare l'handle dell'oggetto `Boolean` che rappresenta i valori `True` o `False`. Questi handle rimangono invariati affinché sia possibile codificarli in modo sicuro. Di seguito sono riportati gli handle:

Active_Boolean_Table	Boolean_Table
actbool:4551 = 'Active'	bool:200 = 'False'
actbool:4552 = 'Inactive'	bool:201 = 'True'

Recupero della lunghezza degli elenchi

Quando si richiedono i valori di attributo da un oggetto, ad esempio utilizzando il metodo `getObjectValues()`, è possibile ottenere la lunghezza di un elenco correlato tramite l'attributo seguente:

```
"<listName>.length"
```

Ad esempio, per ottenere il numero di registri attività per una richiesta specifica, passare al metodo `getObjectValues()` quanto riportato di seguito:

```
"act_log_all.length"
```

Nota: questo è l'unico modo per utilizzare i nomi degli elenchi in questi tipi di metodi.

Capitolo 10: Integrazione con altri prodotti

È possibile integrare CA Service Desk Manager con alcuni prodotti CA, tuttavia non verranno fornite informazioni dettagliate sulle integrazioni con tutti i prodotti CA.

Nota: per informazioni dettagliate sulle integrazioni aggiuntive con CA Service Desk Manager non descritte in questa sezione, vedere il *CA Unicenter Service Desk Integrations Green Book* all'indirizzo <http://ca.com/support>.

Questa sezione contiene i seguenti argomenti:

[Integrazione di CA Workflow](#) (a pagina 521)

[Integrazione di CA NSM](#) (a pagina 526)

[Integrazione di Portale CA](#) (a pagina 571)

[Integrazione di prodotti Mainframe](#) (a pagina 578)

[Integrazione di CA Service Desk Manager con SAP Solution Manager](#) (a pagina 582)

Integrazione di CA Workflow

Un flusso di lavoro definisce le attività, le procedure, le organizzazioni o i singoli individui coinvolti, le informazioni di input e output richieste e gli strumenti necessari per la gestione di ciascuna operazione in un processo aziendale. Il servizio CA Workflow fornisce una soluzione completa per la gestione dei processi di business.

Di norma, per *flusso di lavoro* si intende l'automazione, parziale o totale, di un processo aziendale durante il quale si verifica il trasferimento di documenti, informazioni o attività da un partecipante all'altro affinché vengano svolte le azioni appropriate nel rispetto di una serie di regole procedurali.

CA Workflow è un sistema modulare e generico di gestione del flusso di lavoro ad elevate prestazioni che consente di definire, gestire ed eseguire i flussi di lavoro e fornisce una soluzione di flusso di lavoro generica.

CA Workflow è integrato in CA Service Desk Manager mediante i servizi Web.

Componenti di CA Workflow

CA Workflow utilizza i componenti seguenti forniti con il kit per l'integrazione dei flussi di lavoro:

- [Workflow Design Environment](#) (a pagina 522)
- [Server Workflow](#) (a pagina 524)
- [Elenco lavori](#) (a pagina 524)

CA Workflow Design Environment

CA Workflow Design Environment consente di creare e gestire i flussi di lavoro. CA Workflow Design Environment rappresenta lo strumento fondamentale per la creazione e la gestione delle definizioni di processo e delle istanze di flusso di lavoro nonché per il controllo dell'interazione tra i partecipanti ai flussi di lavoro.

Una società crea un processo aziendale per identificare le risorse, le attività manuali e automatizzate e le relazioni tra le attività per il raggiungimento degli obiettivi aziendali. Un flusso di lavoro automatizza, parzialmente o per intero, il processo aziendale definendo le attività del processo nella definizione di un processo. Generalmente, tali attività includono il trasferimento di moduli, attività o informazioni da una risorsa all'altra (per risorsa si intende l'utente o il software).

La definizione di un processo è una rappresentazione del processo aziendale. Tale definizione è composta da nodi, eventi, ruoli, attori, lavoro e dai criteri per l'avvio e l'interruzione del processo.

Mentre le definizioni di processo rappresentano le attività future desiderate per il processo aziendale, le istanze di processo rappresentano le attività in corso. Tramite l'esecuzione di una definizione di processo, è possibile creare un'istanza di processo. È possibile creare più istanze di processo della stessa definizione di processo, definita anche istanza di definizione di processo.

Avvio di CA Workflow Design Environment (Windows)

In qualsiasi momento è possibile avviare CA Workflow Design Environment per creare e gestire flussi di lavoro. Per avviare CA Workflow Design Environment, selezionare Start, Programmi, CA, Service Desk, CA Workflow IDE.

Nota: è anche possibile avviare CA Workflow Design Environment facendo doppio clic sul file *ide.bat* che si trova nella directory `$NX_ROOT\site\Workflow\Client`. Se la variabile classpath IDE richiede aggiunte per soddisfare i requisiti dell'applicazione, è necessario modificare il parametro APPCPATH nel file *ide.bat* e utilizzarlo per richiamare l'IDE.

Avvio di CA Workflow Design Environment (Linux)

In qualsiasi momento è possibile avviare CA Workflow Design Environment per creare e gestire flussi di lavoro. Per avviare CA Workflow Design Environment, eseguire il file *ide.sh* disponibile nella directory `$NX_ROOT/site/Workflow/Client`. CA Workflow IDE non è supportato in UNIX.

Nota: per soddisfare i requisiti delle applicazioni, il file *ide.sh* include un parametro `APPCPATH` che è possibile modificare per l'aggiunta a classpath.

Parametri IDE CA Workflow

Quando si accede a CA Workflow Design Environment, viene visualizzata una schermata di accesso. In tale schermata sono già inseriti dati relativi a nome utente, password e connessione URL. Per semplificare l'accesso all'IDE, è possibile ignorare completamente questa schermata utilizzando la combinazione desiderata dei parametri seguenti:

```
-u <nomeutente>  
-p <password>  
-url <URL PM>  
-t <token sessione protetta eIAM>
```

È possibile richiamare l'IDE specificando un nome utente e la password (-u e -p) oppure un token (-t). Il token -t fa riferimento a una sessione protetta esportata (definita anche artefatto), corrispondente a una stringa. Ciò consente ai prodotti principali di riutilizzare qualsiasi sessione protetta esistente anziché dover richiedere nuovamente la password e il nome utente.

Il parametro -url deve essere specificato obbligatoriamente indipendente dal fatto che si utilizzi il metodo combinato ID utente/password -u e -p o il metodo token -t.

Ad esempio, [-u, -p, -url] o [-t, -url]

Per utilizzare questa funzionalità per ignorare la schermata di accesso all'IDE, modificare il file *ide.bat* (per Microsoft Windows) o *ide.sh* (per Linux) per aggiungere questi parametri all'elenco dei parametri comunicati al comando Java.

Nota: questa funzionalità può essere utilizzata con il file *ide.exe*.

Server CA Workflow

Il server CA Workflow mostra l'esecuzione runtime e i servizi di gestione per i processi del flusso di lavoro. Il server CA Workflow è costituito dai componenti seguenti:

- Actor Adapters, per l'espansione delle attività del flusso di lavoro
- Process Engine, per l'esecuzione delle istanze di definizione di processo
- Gestione processi, che consente la gestione delle definizioni e delle istanze di processo

Tutti i client del flusso di lavoro, Progettazione processo, Elenco di lavoro e l'interfaccia API dei servizi Web e Java utilizzano i servizi forniti dal server CA Workflow.

Elenco lavori

È possibile richiamare l'applicazione Elenco di lavoro tramite un browser Web (ad esempio, `http://<nomehost>:<numero porta>/wl`) o tramite chiamate API da un prodotto incorporato.

Accesso CA Workflow

CA Service Desk Manager consente di gestire il flusso di lavoro grazie ad un motore del flusso di lavoro comune. Questo sistema per i flussi di lavoro mette a disposizione un ambiente di definizione dei flussi di lavoro, meccanismi di diramazione sofisticati e la possibilità di interagire con singoli utenti che non hanno accesso diretto all'applicazione CA Service Desk Manager per ottenere le approvazioni. È possibile utilizzare l'autenticazione CA Workflow e aggiungere utenti ai gruppi di CA Workflow.

CA EEM e CA Workflow

Tutti gli accessi a CA Workflow sono autenticati da CA EEM. Per accedere all'Elenco lavori o all'IDE CA Workflow, un utente deve disporre di un record utente CA EEM. L'amministratore di CA Workflow specificato durante la configurazione di CA Service Desk Manager dispone dell'accesso completo a CA Workflow. Per impostazione predefinita, questo amministratore viene utilizzato da CA Service Desk Manager per l'integrazione di CA Workflow. Questo account utente viene impostato tramite le opzioni `cawf_username` e `cawf_password` in Gestore opzioni. È necessario accertarsi che il nome utente e la password impostati in queste opzioni siano corretti e che l'utente disponga di accesso completo alle risorse di CA Workflow all'interno di CA EEM.

Classi di risorse

CA Workflow utilizza inoltre CA EEM per limitare l'accesso a specifiche funzioni di CA Workflow. L'accesso viene controllato da due classi di risorse:

IDE

La risorsa IDE è dotata di un'unica azione denominata *accesso* per accedere all'IDE. Per accedere all'applicazione CA Workflow IDE, l'utente deve disporre dell'autorizzazione.

Processo

La risorsa Processo è dotata di un'unica azione denominata *avvio* per avviare un'istanza di processo. Per avviare i processi dell'applicazione Web Elenco di lavoro, è necessario disporre dell'autorizzazione. Tutti gli utenti dispongono di accesso all'applicazione CA Workflow Worklist per visualizzare ed eseguire attività degli elementi di lavoro. Questa autorizzazione consente solo di avviare nuove istanze dall'applicazione Elenco di lavoro.

Nota: queste classi di risorse vengono definite con l'istanza dell'applicazione CA Service Desk Manager in CA EEM. Quando si accede all'interfaccia utente Web di CA EEM, è necessario specificare l'istanza dell'applicazione CA Service Desk Manager per visualizzare le risorse, i criteri e i gruppi descritti in questa sezione.

Aggiunta di utenti ai gruppi di CA Workflow

Gli utenti che devono accedere all'IDE o avviare le istanze di processo hanno bisogno di un'autorizzazione per le risorse e le due azioni. La configurazione di CA Service Desk Manager aggiunge due norme a CA EEM, che garantiscono l'accesso a tali risorse. Sono aggiunti anche due gruppi di utenti dotati dei diritti per le norme: gli amministratori CA Workflow e gli iniziatori del processo CA Workflow. L'aggiunta di utenti al gruppo degli amministratori di CA Workflow consente loro l'accesso all'IDE. L'aggiunta di utenti al gruppo di iniziatori dei processi di CA Workflow consente loro di avviare i processi dall'applicazione Elenco di lavoro.

Per aggiungere/rimuovere utenti nei gruppi del computer in cui è installato CA EEM

1. Selezionare Start, Programmi, CA, Embedded Entitlements Manager, EEM UI.

Viene visualizzata la finestra di accesso.

2. Selezionare l'applicazione CA Service Desk Manager e immettere la password e il nome dell'amministratore di CA EEM.

Viene visualizzata la finestra principale di CA EEM.

3. Selezionare Gestisci identità.
4. Selezionare il tipo di ricerca Utenti, immettere i criteri di ricerca e fare clic su Cerca.
5. Selezionare un utente dall'elenco dei risultati.
6. Nella finestra dei dettagli dell'utente, aggiungere o rimuovere l'adesione al gruppo nella sezione Adesione gruppi applicazione.

Se la sezione non viene visualizzata, fare clic su Aggiungi informazioni su utente applicazione.

7. Fare clic su Salva.

Gli utenti vengono aggiunti ai gruppi.

Integrazione di CA NSM

L'integrazione di CA NSM comporta l'installazione automatica se il server CA Service Desk Manager e CA NSM sono installati nello stesso computer.

Windows

Quando il server CA Service Desk Manager e CA NSM sono installati in computer diversi, è necessario installare e configurare nel server CA NSM anche un server CA Service Desk Manager secondario oppure il componente dell'integrazione di CA NSM autonomo.

UNIX

Quando il server CA Service Desk Manager e CA NSM sono installati in computer diversi, è necessario installare un server CA Service Desk Manager secondario nel server CA NSM.

L'integrazione di CA NSM consente inoltre di effettuare le operazioni seguenti:

- Controllare automaticamente eventuali problemi di gestione della rete rilevati da CA NSM Event and Alert Management.
- Coordinare automaticamente gli eventi di gestione critici rilevati da CA NSM con la gestione degli incidenti
- Stabilire l'impatto degli amministratori di rete e del personale dell'assistenza clienti.
- Evitare un numero eccessivo di richieste o di incidenti.
- Aggiornare automaticamente le richieste o gli incidenti.
- Implementare le regole aziendali come procedure ottimali per la gestione della rete e del supporto dei servizi.
- Inviare automaticamente richieste o incidenti nuovi.

- Automatizzare l'interazione con CA Service Desk Manager per ridurre il carico di lavoro del personale dell'assistenza tecnica eliminando alcune attività manuali
- Ridurre il numero di richieste e di incidenti aperti dagli utenti quando si verifica un problema nell'azienda, poiché le richieste o gli incidenti vengono creati automaticamente non appena si verifica il problema

Modalità di integrazione con CA NSM

Completare la procedura seguente per integrare CA Service Desk Manager e CA NSM:

1. Assicurarsi che CA Service Desk Manager e CA NSM siano stati installati e configurati correttamente.

Importante Se quando si esegue l'integrazione di CA Service Desk Manager con CA NSM si cambiano le impostazioni predefinite, si potrebbero ottenere risultati indesiderati. Ad esempio, per evitare la creazione istantanea di migliaia di richieste di CA Service Desk Manager durante l'integrazione, i parametri seguenti inclusi nel file NX.env che si trova nella directory \$NX_ROOT (UNIX) o nella directory-installazione (Windows) sono impostati sul valore predefinito NO:

```
@NX_TNG_OBJECT_UPDATED_SUBSCRIBE=NO
@NX_TNG_OBJECT_ADDED_SUBSCRIBE=NO
@NX_TNG_OBJECT_DELETED_SUBSCRIBE=NO
@NX_TNG_OBJECT_STATUS_UPDATED_SUBSCRIBE=NO
```

2. Integrare CA Service Desk Manager e CA NSM.
3. Creare asset di proprietà.
4. Monitorare i messaggi della console degli eventi.
5. Filtrare gli eventi non necessari.
6. Risolvere i problemi relativi all'integrazione, se necessario.

Ulteriori informazioni:

[Creazione di asset di proprietà](#) (a pagina 530)

[Modalità di monitoraggio dei messaggi della console degli eventi](#) (a pagina 531)

[Considerazioni sulle regole di filtro](#) (a pagina 532)

[Risoluzione degli errori di integrazione](#) (a pagina 557)

Configurare il convertitore in UNIX

Dopo l'integrazione di CA Service Desk Manager e CA NSM, occorre configurare anche il convertitore utilizzando l'utilità `pdm_edit` come segue:

1. Nell'installazione del server primario CA Service Desk Manager, accedere alla directory `$NX_ROOT/samples/pdmconf`.
2. Immettere il comando seguente per avviare l'utilità `pdm_edit`:
`pdm_perl pdm_edit.pl`
3. Rispondere alle richieste in base alle proprie esigenze e, quando viene visualizzato il menu principale, immettere **N** per selezionare l'opzione Modifica convertitori UNI (UNIX_ONLY).
4. Selezionare **A** per aggiungere, quindi immettere il nome o l'indirizzo IP del server CA NSM (configurato come server secondario di CA Service Desk Manager) quando viene richiesto di specificare un nome host.
5. Lo script richiede di specificare un indirizzo IP. Immettere l'indirizzo IP del server primario CA Service Desk Manager.
6. Premere Invio per tornare al menu principale e immettere **X** per salvare e chiudere.

Questo processo crea un file denominato `pdm_startup.rmt` che memorizza i nuovi valori di configurazione.

7. Creare un backup del file `pdm_startup.tpl` che si trova nella directory `$NX_ROOT/pdmconf` dell'installazione del server primario CA Service Desk Manager, quindi sostituirlo con il file `pdm_startup.rmt` appena creato.
8. Eseguire `pdm_configure` sul server primario CA Service Desk Manager senza apportare alcuna modifica. Le nuove impostazioni di configurazione vengono attivate al successivo avvio del server CA Service Desk Manager.

Importante non reinizializzare il database durante la riconfigurazione.

9. Come utente con privilegi, eseguire `pdm_proctor_init` sul server CA NSM per avviare il proctor CA Service Desk Manager.
10. Come utente con privilegi, riavviare i servizi di CA Service Desk Manager per avviare i relativi daemon. Eseguire `pdm_status` per visualizzare lo stato dei daemon.

Prendere in considerazione quanto segue quando si effettuano le selezioni durante il processo di integrazione:

- Prima che il processo di "ricezione di un evento NSM e creazione di una richiesta in CA Service Desk Manager" possa funzionare, è necessario installare e configurare tutti i componenti e accertarsi che siano attivi.
- Un evento va perduto se viene interrotto il servizio Event Converter. Tale servizio mette in coda gli eventi CA NSM quando il sistema CA Service Desk Manager è in pausa (ovvero, non ne è stata interrotta l'esecuzione dal pannello Servizi di Microsoft Windows). Al riavvio di CA Service Desk Manager, il sistema elabora gli eventi in coda.
- Il numero massimo di eventi che possono essere messi in coda dal servizio CA NSM Event Converter è indicato dalla variabile di ambiente `NX_TNGCNV_QUEUE_SIZE`.
- Quando viene ricreato il repository CA NSM dopo l'integrazione con CA Service Desk Manager, le voci di menu di CA Service Desk Manager vengono perse. Per ripristinarle, è necessario eseguire nuovamente l'integrazione sul computer Windows di CA NSM. A tale scopo, eseguire il file `integAHD.exe` che si trova nella directory *directory-installazione\bin*.
- Se si avvia il servizio CA NSM Event Converter durante la generazione di eventi CA NSM, gli eventi che si verificano prima dell'avvio del convertitore vengono persi.

Processo di post-integrazione

Dopo l'integrazione, attenersi alla procedura riportata di seguito:

1. Creare gli asset di proprietà di CA Service Desk Manager che rappresentano oggetti gestiti da WorldView.
2. Monitorare i messaggi della console degli eventi per definire i record messaggio e le azioni dei messaggi necessari per la creazione automatica delle richieste.
3. Creare le voci necessarie nel file `topology.cfg` e definire le regole di filtro e del writer per filtrare gli eventi indesiderati.
4. Eseguire la risoluzione dei problemi, se necessario.

Ulteriori informazioni:

[Creazione di asset di proprietà](#) (a pagina 530)

Creazione di asset di proprietà

Numerosi prodotti CA creano asset nell'CA MDB, tuttavia, non diventano automaticamente disponibili per CA Service Desk Manager. Generalmente in un'organizzazione CA Service Desk Manager si ha necessità di tenere traccia solo degli asset di proprietà dell'organizzazione, acquistati tramite un processo formale. È molto probabile che alcuni dispositivi rilevati sulla rete da altri prodotti CA non diventino automaticamente disponibili per CA Service Desk Manager. Ad esempio, il computer laptop di un consulente in visita potrebbe non interessare affatto l'organizzazione CA Service Desk Manager.

Per rendere disponibile un asset rilevato nell'CA MDB per CA Service Desk Manager, utilizzare la finestra di selezione Asset rilevati, cui è possibile accedere dal modulo Ricerca asset o Crea nuovo asset nell'interfaccia Web per gli analisti.

Nota: la finestra di selezione Asset rilevati è disponibile sul client Web.

Se si utilizza l'integrazione WorldView, è possibile rendere gli asset rilevati disponibili per CA Service Desk Manager dall'utilità della riga di comando `pdm_nsmimp`. Unicenter Explorer e la mappa 2D/3D Unicenter NSM consentono di visualizzare e creare richieste facendo clic con il pulsante-destro del mouse su un oggetto gestito per visualizzare due opzioni di menu: Crea richiesta ed Elenco richieste. Tali opzioni vengono aggiunte a CA NSM durante il processo di integrazione con CA Service Desk Manager.

Modalità di registrazione di asset rilevati

L'utilità `pdm_discimp` consente la registrazione batch degli asset rilevati non CA Service Desk Manager. Viene utilizzata per cercare nell'CA MDB gli asset registrati da altri prodotti software e registrarli come asset CA Service Desk Manager affinché possano essere utilizzati in CA Service Desk Manager. Rappresenta un processo batch interattivo.

Funziona in modo simile alla finestra di dialogo Asset rilevati che può essere avviata dal modulo Web Ricerca/Elenco asset. Questo programma esegue una query nelle tabelle `ca_logical_asset`, `ca_asset` e `ca_logical_asset_property` utilizzando diversi parametri e tenta di registrare i nuovi asset CA Service Desk Manager utilizzando i valori rilevati.

Nota: se l'elaborazione restituisce un'etichetta asset vuota, viene utilizzato il valore rilevato per il nome host o il nome DNS. È necessario che gli asset abbiano almeno un'etichetta e una classe asset da registrare per l'uso in CA Service Desk Manager.

A causa della struttura dell'CA MDB e dell'architettura di CA Service Desk Manager, vengono eseguite le query seguenti per selezionare i record appropriati per l'elaborazione.

1. Una query recupera dalle tabelle `ca_logical_asset` e `ca_asset` le righe corrispondenti all'etichetta, al numero di serie, al tag e al nome host.
2. Per ogni riga risultante, viene eseguita una query nella tabella `ca_logical_asset_property` per verificare la corrispondenza per `dns_name` e `mac_address`.

L'asset rilevato dalla prima query viene selezionato per la registrazione quando la seconda query restituisce delle righe.

Nota: questo processo può influire sulle prestazioni.

Modalità di monitoraggio dei messaggi della console degli eventi

L'installazione CA Service Desk Manager di base esegue automaticamente il monitoraggio delle variazioni dello stato degli oggetti monitorati e dell'aggiunta di nuovi oggetti gestiti. È possibile configurare l'ambiente per utilizzare AHD.DLL per il monitoraggio dei messaggi della console su Windows e l'invio dei messaggi di evento al server CA Service Desk Manager.

È consigliabile utilizzare AHD.DLL per inviare gli eventi a CA Service Desk Manager. Tuttavia, sono disponibili altri metodi quando la console degli eventi è in esecuzione su un sistema UNIX.

La funzione Gestione eventi in CA NSM consente di identificare gli eventi ai quali si desidera rispondere e di specificare una o più azioni da avviare automaticamente. Dopo aver definito un messaggio e un'azione a esso associata, l'azione viene eseguita automaticamente a ogni rilevamento dell'evento.

Dopo l'integrazione con CA Service Desk Manager, quando si verifica il messaggio di evento, è possibile inviare dati di eventi generici a CA Service Desk Manager per:

- Creare nuove richieste o aggiornare richieste esistenti
- Creare e pubblicare annunci sul segnapunti di CA Service Desk Manager

Per iniziare l'integrazione, effettuare le operazioni seguenti:

1. Creare un record msg_action CA NSM utilizzando AHD.DLL.
2. Trasferire il record dei messaggi alla console degli eventi utilizzando il comando cawto.

Nota: utilizzare le regole dei writer e di filtro predefinite fornite con CA Service Desk Manager finché non si è certi della perfetta integrazione del sistema. Non modificare o rimuovere le regole predefinite finché gli eventi CA NSM non creano le richieste.

Invio di eventi generici (solo UNIX)

Per inviare dati di evento generici ai daemon di filtri in CA Service Desk Manager, utilizzare il daemon uniconv in un'azione messaggio di CA NSM Event Management.

Quindi, i dati di eventi generici possono essere utilizzati per generare richieste automaticamente nello stesso modo in cui AHD.DLL viene utilizzato su Windows. Si tratta del metodo consigliato per UNIX.

Pubblicazione automatica degli annunci

Dopo aver integrato CA Service Desk Manager con CA NSM, è possibile creare e pubblicare annunci sul contatore di CA Service Desk Manager da CA NSM.

Considerazioni sulle regole di filtro

Una volta che è stata configurata correttamente l'integrazione e che gli eventi creano o aggiornano le richieste come definito, è possibile modificare le regole che consentono di filtrare gli eventi non desiderati.

L'elenco seguente fornisce alcuni suggerimenti per la codifica delle regole di filtro:

- Riavviare CA Service Desk Manager ogni volta che si cambia una regola di filtro.
- Utilizzare le regole dei writer predefinite durante il controllo delle regole di filtro.
- Durante la codifica dei parametri *node_ID*, *user_ID* o *event_ID* nella regola di filtro, è necessario rispettare l'uso di maiuscole e minuscole dell'evento in arrivo. Per assicurarsi che siano state utilizzate correttamente maiuscole e minuscole, creare un evento in CA NSM relativo al parametro di cui si esegue il controllo. In questo modo, viene creata una richiesta con le informazioni necessarie. Per la richiesta, utilizzare lo stesso carattere della regola di filtro. Tra l'altro, corrisponde anche al carattere dei messaggi in arrivo della console.

- Quando si codifica una regola del filtro per uno specifico evento, il testo in arrivo in corrispondenza dell'evento potrebbe avere il seguente formato: "Object_Status_Updated minor." Codificare la regola del filtro come indicato di seguito:

```
tng::*::*:Object_Status_Updated.*minor.*::(0,1)
```

- Gli spazi nell'evento possono essere caratteri non stampabili. È necessario codificare il filtro in modo da includere uno o più caratteri con un punto o un asterisco (.*) anziché con lo spazio (' '). Aggiungere inoltre .* alla fine dell'evento per qualsiasi carattere non stampabile che può trovarsi alla fine del testo dell'evento.
- Per accertarsi che il filtro funzioni durante la codifica di più parametri in esso contenuti, quale la combinazione di parametri *node_ID*, *user_ID* e *event_ID*, è necessario codificare solo il parametro da cui si desidera iniziare e verificarne il corretto funzionamento. Aggiungere, quindi, il parametro successivo e controllare che funzioni insieme all'altro parametro e così via fino alla fine.
- Per semplificare il debug, ordinare le regole di filtro inserendo la più specifica all'inizio del file e procedendo fino a quella più generica alla fine del file.

Le regole dei writer degli eventi seguono le stesse pratiche di debug delle regole di filtro. Se si utilizza l'azione CR_CREATE ed è stato incluso un modello, verificare che il modello esista realmente.

Modalità di filtraggio automatico degli eventi

È possibile configurare CA Service Desk Manager per la creazione automatica di richieste di messaggi di evento ed errore generate tramite dispositivi di rete e altre origini di eventi. La definizione della modalità di filtro degli eventi consente di rilevare automaticamente il verificarsi di un evento e di eseguire le azioni appropriate per poterlo gestire. Questo metodo può migliorare l'efficienza operativa generale e ridurre il rischio di errori.

È possibile configurare CA Service Desk Manager per l'esecuzione delle operazioni seguenti:

- Filtrare gli eventi in base all'host, al contenuto, al tipo e ad altre informazioni fornite da CA NSM
- Creare automaticamente richieste per messaggi di errore ed evento generati tramite dispositivi di rete
- Eseguire automaticamente comandi in risposta a un evento

Per filtrare gli eventi automaticamente, effettuare le operazioni seguenti:

- Definire le regole di filtro per l'identificazione degli eventi che richiedono una gestione particolare
- Definire le regole dei writer degli eventi per l'identificazione delle azioni da eseguire automaticamente al rilevamento degli eventi

Le regole di filtro e dei writer degli eventi utilizzano una struttura di dati di eventi generici per la ricezione e l'invio di dati. Vengono definiti tramite un editor di testo e memorizzati e modificati solo sul server CA Service Desk Manager.

Qualsiasi evento è idoneo per l'elaborazione tramite le regole di filtro e dei writer degli eventi. Di seguito sono riportati alcuni esempi di eventi che è possibile elaborare tramite le regole di filtro e dei writer degli eventi:

- Errori hardware
- Errori di processi batch pianificati
- Uso eccessivo della CPU
- Frequenze di paging elevate
- Attività file insolita
- Condizioni di protezione insolite

È possibile configurare qualsiasi numero di daemon di filtri, daemon dei writer degli eventi e origini di eventi su computer diversi. Le posizioni e le relazioni di questi elementi vengono memorizzate nel file della topologia sul server CA Service Desk Manager.

Nota: quando è integrato in CA NSM, è possibile utilizzare il daemon `uniconv` per la generazione automatica delle richieste (questo è il metodo preferito per UNIX). `uniconv` viene utilizzato in un'azione messaggio in CA NSM Event Management.

Dati di eventi generici

Le informazioni relative agli eventi vengono comunicate tramite una struttura di dati di *eventi generici*. La struttura dei dati di eventi generici è costituita dai seguenti elementi:

Tipo di origine

Indica il formato per il resto dell'evento.

ID nodo

Indica l'ID o il nome del dispositivo.

ID utente

Indica l'ID o il nome utente (quando applicabile).

Origine principale

Indica l'ID applicazione di origine.

Origine secondaria

Indica l'agente dell'evento o l'ulteriore definizione.

Data e ora

Indica la data e l'ora dell'evento.

ID evento

Indica la stringa evento di origine che ha attivato l'evento.

Dati evento

Indica i dati di eventi associati.

Gravità

Indica l'importanza dell'evento.

Handle

Indica la stringa fornita dal daemon risultante dalle regole.

Origine handle

Indica l'identificativo daemon che ha assegnato l'handle.

Stato handle

Indica lo stato come Crea, Aggiorna o Interrompi.

Conteggio stato

Indica il numero di aggiornamenti.

Impostazione della regola di filtro

I filtri ricevono informazioni dalle origini degli eventi e le inviano ai writer degli eventi. Poiché i dispositivi di rete generano centinaia di messaggi di evento, è possibile utilizzare le regole di filtro per isolare quelli utilizzabili per la creazione di richieste. Grazie alle regole di filtro è possibile:

- Determinare i trap o gli eventi di rete da segnalare e il metodo di segnalazione.
- Controllare ciò che accade con la segnalazione di ciascun tipo di trap o evento. Tra le azioni consentite vi è la possibilità di ignorare, segnalare e contrassegnare.

Quando è integrato in CA NSM, il filtraggio consente di gestire gli eventi di tutti i sistemi gestiti mediante CA NSM, incluse le reti TCP/IP e SNA.

Grazie al filtraggio degli eventi, è possibile recuperare specifiche informazioni su un determinato nodo, utente o workstation e passarle ai writer degli eventi. È possibile definire regole di filtro degli eventi in base alle proprie esigenze per poter identificare gli eventi sospetti e correggerli prima che causino problemi.

Nota: quando si scrivono regole di filtro è utile acquisire familiarità con le espressioni regolari UNIX. È anche possibile utilizzare le espressioni regolari UNIX su Windows.

Definizioni della regola di filtro

Le regole di filtro utilizzano la corrispondenza delle espressioni regolari UNIX per determinare se un evento dispone di una regola di filtro di corrispondenza e blocca gli eventi non conformi al filtro. Un filtro speciale (ID=5) comunica al writer l'evento generico in arrivo non modificato. Il filtro fa passare solo gli eventi filtrati e assegna una fonte handle di *filtro* e lo stato handle di *creazione, aggiornamento o interruzione*.

CA Service Desk Manager utilizza i campi Origine principale, ID evento e ID utente della struttura di dati di eventi generici per individuare una regola di filtro di corrispondenza.

Importante Le regole di filtro comunicano gli eventi a un altro daemon che utilizza le regole dei writer degli eventi, che consentono di creare automaticamente le richieste.

Il file delle regole di filtro predefinito, `tngfilter_rule.dat`, si trova nella directory `$NX_ROOT/site/eh/IP` (UNIX) o nella directory *directory-installazione*\site\eh\IP (Windows) sul server CA Service Desk Manager. La directory `$NX_ROOT` o *directory-installazione* corrisponde alla directory in cui è stato installato CA Service Desk Manager, mentre *IP* corrisponde all'indirizzo IP del computer in cui si trova il filtro. Generalmente, si tratta del server CA Service Desk Manager.

Questo file contiene molte righe di commento che descrivono come configurare diverse regole di filtro. Le righe di commento iniziano con il segno di cancelletto (`#`).

Utilizzare un editor di testo per visualizzare, aggiornare e salvare il file delle regole di filtro. Tuttavia, non utilizzare un editor che lascia i caratteri di formattazione extra nel file. Si consiglia WordPad per gli utenti Windows e vi per gli utenti UNIX.

Sintassi (regole di filtro)

La sintassi delle regole di filtro è la seguente:

```
source_type::node_ID::user_ID::event_ID::filter
```

dove:

I campi nella regola sono separati da tre caratteri di due punti (:::). È possibile utilizzare un asterisco (*) come carattere jolly, per indicare che il valore del parametro viene ignorato quando si stabilisce se un evento in arrivo corrisponde al criterio della regola di filtro.

Nota: i primi quattro parametri nella regola di filtro descrivono un criterio in base al quale misurare gli eventi in arrivo. Tale criterio viene utilizzato per determinare se il filtro specificato nell'ultimo parametro della regola deve elaborare un evento in arrivo.

Parametri (regole di filtro)

source_type

Specifica il tipo di origine che indirizza gli eventi al filtro. Il campo Origine principale dell'evento in arrivo viene confrontato con il valore in questo parametro. Generalmente, il valore di questo parametro viene determinato dal tipo di converter che invia gli eventi al filtro. I valori validi sono:

uni

Identifica il convertitore CA NSM di UNIX.

tng

Identifica il convertitore CA NSM di Windows.

Se un evento in arrivo corrisponde a diverse regole durante il confronto dei tipi di origine e degli ID evento, vengono confrontati gli ID nodo.

node_ID

Specifica l'ID del nodo in cui viene generato l'evento. Questo parametro deve corrispondere esattamente all'ID nodo dell'evento in arrivo; in caso contrario, questa regola di filtro non viene utilizzata. Un asterisco (*) indica che l'ID nodo viene ignorato quando si determina se un evento in arrivo corrisponde a questo criterio della regola di filtro.

Le regole che corrispondono all'ID nodo dell'evento in arrivo hanno la precedenza sulle regole per le quali è specificato un asterisco (*) per l'ID nodo.

Se un evento in arrivo corrisponde a diverse regole durante il confronto dei tipi di origine, degli ID evento e degli ID nodo, vengono confrontati gli ID utente.

user_ID

Indica un utente associato all'evento. Utilizzare questo parametro per eseguire un'azione particolare per gli eventi relativi a un utente specifico. Molti eventi non sono associati a specifici utenti. Questo parametro non può contenere un'espressione regolare UNIX. È necessario specificare un asterisco o un ID utente esatto. Un asterisco (*) è l'impostazione predefinita e indica che l'utente viene ignorato durante la selezione della regola.

Le regole che corrispondono all'ID utente associato all'evento hanno la precedenza sulle regole per le quali è specificato un asterisco (*) per l'ID utente.

event_ID

Specifica l'ID dell'evento. È anche possibile utilizzare un'espressione regolare UNIX. Un punto e un asterisco (.*) consentono la corrispondenza con qualsiasi nome di evento. Ad esempio, è possibile specificare [Aa].* per consentire la corrispondenza con qualsiasi evento che inizia con la lettera "a", minuscola o maiuscola.

Se il parametro *event_ID* è costituito da testo semplice (non un'espressione regolare), deve corrispondere esattamente all'ID dell'evento generico. Una corrispondenza parziale non viene considerata. Se il parametro *event_ID* è un'espressione regolare, viene utilizzata la corrispondenza della lunghezza dell'espressione regolare per determinare il livello di corrispondenza tra l'*event_ID* della regola di filtro degli eventi e l'ID dell'evento generico.

Se un evento in arrivo corrisponde a diverse regole durante il confronto dei tipi di origine e degli ID evento, vengono confrontati gli ID nodo.

filter

Specifica il filtro da utilizzare per l'elaborazione dell'evento in arrivo e i parametri usati dal filtro. Il formato è il seguente:

(filter_id, filter_parameter1, filter_parameter2...)

I valori validi per *filter_id* sono:

Valore=0

Segnala tutti gli eventi

Valore=2

Ignora gli eventi che si verificano di rado

Valore=3

Ignora le interruzioni più brevi della lunghezza specificata in *filter_parameter1*

Valore=4

Ignora i burst più brevi della lunghezza specificata in *filter_parameter1*

Valore=5

Passa tutti gli eventi alla destinazione senza modifica

Il numero di parametri di filtro varia per ciascun *filter_id* come indicato dalla tabella seguente:

filter_ID	filter_parameter1	filter_parameter2	filter_parameter3
0	0=no, 1=sì. Indica se gli eventi devono essere segnalati come problemi separati.	None	None
2	N. di occorrenze Specifica quante volte un evento deve verificarsi in un determinato intervallo di tempo per essere considerato importante.	Intervallo Specifica l'intervallo di tempo, in secondi, nel quale deve verificarsi un evento per essere considerato importante.	0=no, 1=sì. Indica se gli eventi devono essere segnalati come problemi separati.
3	Intervallo Specifica l'intervallo di tempo, in secondi, nel quale deve verificarsi un evento per essere considerato importante.	0=no, 1=sì. Indica se gli eventi devono essere segnalati come problemi separati.	None
-4	Intervallo Specifica l'intervallo di tempo, in secondi, nel quale deve verificarsi un evento per essere considerato importante.	0=no, 1=sì. Indica se gli eventi devono essere segnalati come problemi separati.	None
5	None	None	None

Nota: i primi quattro parametri nella regola di filtro descrivono un criterio in base al quale misurare gli eventi in arrivo. Tale criterio viene utilizzato per determinare se il filtro specificato nell'ultimo parametro della regola deve elaborare un evento in arrivo.

Writer eventi

I writer degli eventi specificano le azioni che devono essere eseguite da CA Service Desk Manager al rilevamento di un evento importante dalla rete. Il writer degli eventi utilizza gli eventi convertiti (che utilizzano la struttura di dati di eventi generici) da una fonte di eventi e gli eventi passati attraverso un filtro per la creazione delle richieste.

Utilizzando i writer degli eventi è possibile:

- Identificare il tipo di evento ricevuto da una fonte di eventi
- Specificare l'azione da eseguire quando il writer degli eventi riceve eventi di questo tipo. Tra le azioni valide vi sono:
 - Creazione di richieste
 - Aggiornamento delle richieste esistenti
 - Esecuzione di un comando
- Indicazione del verificarsi o meno della registrazione

Definizioni delle regole dei writer degli eventi

Quando è installato CA Service Desk Manager, viene fornita una configurazione predefinita per l'esecuzione sul server CA Service Desk Manager. Tale configurazione predefinita imposta un'unica origine di eventi, un filtro e un writer e dispone di una regola di filtro per far passare tutti gli eventi al writer. La regola di filtro predefinita crea le richieste per tutti gli eventi ricevuti.

Il file delle regole dei writer predefinito, `tngwriter_rule.dat`, si trova nella directory `$NX_ROOT/site/eh/IP` (UNIX) o nella directory *directory-installazione*\site\eh\IP (Windows) sul server CA Service Desk Manager. `$NX_ROOT` o *directory-installazione* è la directory in cui è stato installato CA Service Desk Manager mentre *IP* è l'indirizzo IP del server CA Service Desk Manager.

È possibile visualizzare il contenuto di questo file per conoscere le definizioni di filtro e i commenti che descrivono il formato delle regole dei writer. I commenti si trovano all'inizio del file, mentre le regole del writer alla fine. Le righe di commento iniziano con il segno di cancelletto (`#`).

Utilizzare un editor di testo per visualizzare, aggiornare e salvare il file delle regole dei writer. Tuttavia, non utilizzare un editor che lascia i caratteri di formattazione extra nel file. Si consiglia WordPad per gli utenti Windows e vi per gli utenti UNIX.

Sintassi (regole dei writer degli eventi)

La sintassi delle regole dei writer degli eventi è la seguente:

```
event_ID::device::user_ID::majorSrc::minorSrc::action::template::  
command::logging::event_token::user_parms
```

dove:

I campi nella regola sono separati da tre caratteri di due punti (:::). È possibile utilizzare un asterisco (*) come carattere jolly, per indicare che il valore del parametro viene ignorato quando si determinano le corrispondenze per la regola del writer degli eventi.

Parametri (regole dei writer degli eventi)

event_ID

Specifica l'identificativo dell'evento al quale si applica la regola del writer degli eventi. È anche possibile utilizzare un'espressione regolare UNIX. Un punto e un asterisco (.*) consentono la corrispondenza con qualsiasi nome di evento. Ad esempio, è possibile specificare [Aa].* per consentire la corrispondenza con qualsiasi evento che inizia con la lettera "a", minuscola o maiuscola.

Se il parametro *event_ID* è costituito da testo semplice (non un'espressione regolare), deve corrispondere esattamente all'ID dell'evento generico. Una corrispondenza parziale non viene considerata.

Se il parametro *event_ID* è un'espressione regolare, viene utilizzata la lunghezza della corrispondenza dell'espressione regolare per determinare il livello di corrispondenza tra l'*event_ID* della regola del writer degli eventi e l'ID dell'evento generico.

device

Specifica il nome dell'oggetto, generalmente un dispositivo o un host associato all'evento. Un punto e un asterisco (.*) è l'impostazione predefinita e indica che l'oggetto di origine viene ignorato durante la selezione della regola.

Se un evento in arrivo corrisponde a diverse regole durante la valutazione dei tipi di origine e degli ID evento, vengono confrontati i dispositivi. Le regole che corrispondono al dispositivo dell'evento in arrivo hanno la precedenza sulle regole per le quali è specificato un asterisco (*) per il parametro *device*.

Se sono state definite regole per l'assegnazione dei nomi dei dispositivi, questo parametro può rivelarsi particolarmente utile. Ad esempio, se i dispositivi che si trovano negli Stati Uniti vengono denominati USxx, è possibile specificare US.* in questo parametro per eseguire una particolare azione del writer per gli eventi provenienti dai dispositivi negli Stati Uniti.

user_ID

Indica un utente associato all'evento. Utilizzare questo parametro per eseguire un'azione particolare per gli eventi relativi a un utente specifico. Molti eventi non sono associati a specifici utenti. Questo parametro non può contenere un'espressione regolare UNIX. È necessario specificare un asterisco o un ID utente esatto. Un asterisco (*) è l'impostazione predefinita e indica che l'utente viene ignorato durante la selezione della regola.

Se un evento in arrivo corrisponde a diverse regole durante la valutazione dei tipi di origine, degli ID evento e dei dispositivi, vengono confrontati gli ID utente. Le regole che corrispondono all'ID utente associato all'evento hanno la precedenza sulle regole per le quali è specificato un asterisco (*) per il parametro *user_ID*.

majorSrc

Visualizza automaticamente il tipo di origine principale che indirizza gli eventi al writer degli eventi. Questo parametro è obbligatorio. Il suo valore è determinato dall'origine degli eventi. Per eventi originati da CA NSM in Windows, il valore deve essere "tng". Per eventi originati da CA NSM in UNIX, il valore deve essere "uni".

minorSrc

Visualizza automaticamente il tipo di origine secondario che indirizza gli eventi al writer degli eventi. Per gli eventi originati da CA NSM, questo parametro contiene il tipo di evento. Utilizzare un asterisco (*) per accettare tutti gli eventi.

azione

Specifica l'azione eseguita quando il writer degli eventi riceve questo tipo di evento utilizzando uno dei valori seguenti:

CR_CREATE

Consente di scrivere una nuova richiesta per ciascun evento.

CR_UPDATE

Consente di aggiornare una o più richieste oppure di creare una richiesta se non vi sono richieste esistenti. Per impostazione predefinita, i record vengono localizzati tramite la corrispondenza degli attributi *log_agent* e *affected_resource*. È possibile ignorare i valori predefiniti specificando un elenco di attributi di richiesta.

CR_UPDATE_ONLY

Consente di eseguire le stesse operazioni di CR_UPDATE, ma non viene creata alcuna richiesta quando non vengono trovate richieste corrispondenti.

COMMAND

Consente di eseguire il comando specificato nel parametro *command*.

Nota: se CA Service Desk Manager non può accedere a una richiesta o a un ordine di cambiamento, tenta nuovamente l'aggiornamento dopo uno specifico intervallo di tempo.

modello

Specifica il nome del modello da utilizzare per creare una richiesta. Questo parametro non è obbligatorio e viene ignorato se l'azione è diversa da CR_CREATE.

Nota: è necessario creare il modello di richiesta prima della definizione della regola.

comando

Specifica il comando da eseguire se il valore del parametro *action* è COMMAND. Gli argomenti di sostituzione, come mostra la tabella seguente, possono essere incorporati nel comando. Gli argomenti vengono sostituiti dai rispettivi valori reali durante l'esecuzione del comando:

&node

Il nome del dispositivo o l'identificativo del nodo

&user

L'ID o il nome dell'utente

&date

La data dell'evento

&time

L'ora dell'evento

&event-id

La stringa evento di origine che ha attivato l'evento

&data

I dati di evento associati

&sev

Il livello di importanza dell'evento

&major-src

L'ID applicazione di origine

&minor-src

Il nome dell'agente o l'ulteriore definizione dell'evento

&handle

La stringa fornita dal daemon derivante dalle regole

&src-handle

L'identificativo daemon che ha assegnato l'handle

&status-handle

Lo stato dell'handle (i valori validi sono Crea, Aggiorna e Interrompi)

registrazione

Specifica se si verifica la registrazione, utilizzando uno dei seguenti valori:

NESSUNO

Si verifica solo la normale registrazione degli errori. NONE è il valore predefinito.

PDM

La registrazione avviene nel registro di CA Service Desk Manager (stdlog.0) nel formato interno per gli eventi generici.

SYS

La registrazione si verifica nel registro syslog UNIX, che può essere inoltrato alla console Unicenter. All'evento viene assegnato un ID messaggio (CAPD 13) per consentirne l'elaborazione dalla console Unicenter.

BOTH

La registrazione avviene nel registro di CA Service Desk Manager (stdlog.0) e nel registro syslog UNIX.

event_token

Tag di 30 caratteri definito dall'utente che identifica una specifica richiesta associata a un *event_id* (messaggio di evento tng) o tutti i messaggi simili a un *event_id*, ad esempio un *event_id* con caratteri jolly. Il parametro *event_token* è un attributo di richiesta archiviato in ogni richiesta generata dall'interfaccia di CA NSM. Se non è specificato alcun *event_token* nella regola del writer, viene utilizzata la stringa "tng_generated". Ciò consente di aggiornare tutte le richieste corrispondenti all'attributo *event_token*. Ad esempio, due diversi messaggi per lo stesso asset possono aggiornare richieste univoche.

Ad esempio, la prima regola del writer indicata di seguito fa in modo che il processo del writer (tngwriter) crei una richiesta di chiamata con un event_token corrispondente a 'SystemCritical' alla ricezione di un evento NSM identificato dalla stringa 'Event1'. La seconda regola del writer fa in modo che il processo del writer aggiorni il valore dello stato su 'CL' per tutte le richieste di chiamata con un event_token corrispondente 'SystemCritical' alla ricezione di un evento NSM identificato dalla stringa 'Event2'.

er_parms

Valori attributi richiesta

Nota: se si utilizzano più coppie parola chiave/valore, separarle inserendo un punto e virgola (;).

Event4...*:~:~:~:ng:...*:~:~:~:CR CREATE.....NONE:.....%ASSIGNEE=mccda04;CUSTOMER=nsn

Elenco di attributi di richiesta per la corrispondenza durante l'aggiornamento dei record richiesta esistenti

La sintassi per l'elenco di attributi per la corrispondenza ha il formato seguente:

%SEARCH=attribute1[, attribute2...], dove SEARCH è una parola chiave fissa e attribute1, attribute2 e così via sono nomi di ATTRIBUTO specificati nel file text_api.cfg.

L'elenco di ricerca degli attributi predefinito corrisponde a "asset_name" (DEVICE o UUID) e LOG_AGENT. La parola chiave SEARCH aggiunge gli attributi (per la corrispondenza) all'elenco di ricerca predefinito. La parola chiave SEARCH_EXPLICIT ignora completamente l'elenco ricerca predefinito. Solo gli attributi conformi alla parola chiave SEARCH_EXPLICIT vengono utilizzati per cercare una richiesta di chiamata.

Ad esempio, la regola del writer indicata di seguito fa in modo che il processo del writer (tngwriter) aggiorni il valore dello stato su "CL" per tutte le richieste di chiamata con il parametro assignee corrispondente a "mccda04" alla ricezione di un evento CA NSM identificato dalla stringa "Event2".

```
Event2:::*:*::tng::*:CR_UPDATE::::NONE::SystemCritical::%SEARCH=ASSIGNEE;%STATU  
S=CL;%ASSIGNEE=mccda04
```

uno degli attributi dell'elenco viene utilizzato per la ricerca se si trova nell'elenco SEARCH o SEARCH_EXPLICIT. Se non si trova nell'elenco di ricerca, viene utilizzato per impostare o aggiornare il valore dell'attributo nella richiesta di chiamata. Non è possibile utilizzare l'attributo per entrambe le funzioni nella stessa regola del writer.

Nota: per ulteriori informazioni su text_api.cfg e su come viene utilizzato in CA Service Desk Manager, consultare la *Guida all'amministrazione*.

Nomi di parametri speciali sostituiti dal valore corrispondente proveniente dalla struttura di eventi CA NSM

È possibile utilizzare i seguenti nomi di parametri speciali nella stringa *user_parms*:

&message

Il testo associato al messaggio CA NSM.

&parm

Il campo Parm AHD.DLL nella schermata Azione messaggio di CA NSM.

&uuid

L'identificativo univoco universale di CA NSM.

&device

Il dispositivo (ad esempio, il nome host) che ha generato il messaggio CA NSM.

&majorsrc

Il tipo di origine principale che indirizza gli eventi al writer degli eventi. Per eventi originati da CA NSM in Windows, il valore è "tng". Per eventi originati da CA NSM in UNIX, il valore è "uni".

&minorsrc

Il tipo di origine secondario che indirizza gli eventi al writer degli eventi.

&node

Il dispositivo (ad esempio, il nome host) che ha generato il messaggio CA NSM.

&addr

L'indirizzo IP dell'host che ha generato il messaggio CA NSM.

&username

Il nome utente sull'host che ha generato il messaggio CA NSM.

&date

Un numero intero che indica quando è stato generato il messaggio CA NSM, a partire dal 1970.

&time

La data e l'ora del messaggio CA NSM, ad esempio mar. 4 luglio 10.23.37 2000.

&severity

La gravità del messaggio CA NSM.

&tag

I dati dei tag associati al messaggio CA NSM.

Ad esempio, la regola del writer seguente fa in modo che il processo del writer (tngwriter) crei una richiesta di chiamata con il parametro "customer" corrispondente al valore del nome utente (&username) del messaggio di evento alla ricezione di un evento NSM identificato dalla stringa 'Event2'.

```
Event2::*:~*:~tng::*:~CR_CREATE:::~:~NONE:::~:%CUSTOMER=&username
```

Utilizzando *event_token* e *user_parms*, è possibile impostare i valori iniziali o aggiornare i valori di tutti gli attributi della richiesta e specificare i campi per la corrispondenza durante l'individuazione dei record da aggiornare. L'unica restrizione è che l'attributo della descrizione non viene mai aggiornato in un record richiesta di chiamata esistente. Se si specificano l'aggiornamento di un record e il campo della descrizione, viene aggiunto al record esistente un registro di attività contenente il testo della descrizione.

Record azione messaggio CA NSM: <parms...> ahd.dll AHD_Call

È inoltre possibile specificare dati (<parms...>) per AHD_Call nel record azione messaggio CA NSM utilizzabili per sostituire il parametro &Parm specificato nel parametro user_parms della regola del writer. Per fare in modo che i dati specificati per AHD_Call vengano elaborati in questo modo, è necessario che i dati (<parms...>) siano preceduti da un carattere "%" e che il "parametro speciale" &Parm sia incluso nel campo user_parms della regola del writer.

Di seguito vengono riportate un'azione messaggio CA NSM e una regola del writer che consentono al processo del writer di creare richieste con il parametro assignee impostato su "mccda04" al momento della ricezione di un evento NSM identificato dalla stringa "Event3".

```
Ahd.dll AHD_Call %ASSIGNEE=mccda04
```

```
Event3::*:~*:~tng::*:~CR_CREATE:::~:~NONE:::~:&Parm
```

È possibile che i clienti di CA Service Desk Manager che eseguono l'aggiornamento da AHD4.5 e versioni precedenti utilizzino già il campo <parms...>, ad esempio, per la corrispondenza delle regole del writer. Questa procedura può essere portata avanti senza alcuna variazione. Se si desidera utilizzare i parametri "vecchi" e "nuovi", è necessario concatenare i parametri <parms..> vecchi e nuovi mediante un carattere "%".

Esempio:

parametri vecchi ahd.dll AHD_Call

ahd.dll AHD_Call %user_parms nuovi

parametri vecchi ahd.dll AHD_Call %user_parms nuovi

I dati che precedono il primo carattere "%" vengono concatenati al messaggio di evento CA NSM posizionato nel campo di descrizione Richiesta chiamata. Questa è la procedura che è stata seguita da CA Service Desk Manager in passato. I dati successivi al primo carattere '%' vengono utilizzati per sostituire il parametro &Parm nel parametro user_parms nella regola del writer.

Sintassi del registro (stdlog.0) di CA Service Desk Manager

La sintassi per le voci nel file stdlog.0 è la seguente:

```
genDate genTime genNode genProc PID level codefile linenum msgID  
::msgDomain\msgNode:: ::msgGenDomain\msgGenUser::domainID  
::msgDate msgTime::eventID arg tag:: ::IPaddr:filter:filterNum  
::majorSrc:: ::msgSrc::msgType::msgSrcNum:: ::platform
```

dove:

I campi nella regola sono separati da tre caratteri di due punti (:::).

genDate

Specifica il mese e il giorno (in base all'orologio del sistema) in cui è stato generato l'incidente del registro.

genTime

Specifica l'ora (in base all'orologio del sistema) in cui è stato generato l'incidente del registro.

genNode

Specifica il nome del nodo che ha generato l'incidente del registro. Generalmente, corrisponde ai primi otto caratteri del nome DNS del nodo che ha generato l'incidente. Questo valore è sempre lo stesso poiché stdlog.0 contiene solo voci dei processi che vengono eseguiti nello stesso nodo.

genProc

Specifica il nome del processo (ad esempio, ehwriter) che ha generato l'incidente del registro. Il nome del processo è dipendente dall'ambiente operativo, ma deve corrispondere al nome che appare nell'elenco dei processi Task Manager (Windows) o nell'output da un comando ps (UNIX).

PID

Specifica l'identificativo di processo numerico dell'elenco dei processi Task Manager (Windows) o nell'output da un comando ps (UNIX). Il PID è critico quando vengono eseguiti più processi con lo stesso nome di processo. Ad esempio, più agenti di database vengono in genere eseguiti contemporaneamente con lo stesso nome di processo.

level

Specifica l'importanza del messaggio stimata dal programmatore. I valori possibili includono FATAL, EXIT, RESTART, SIGNIFICANT, SEVERE, ERROR, MINIMUM, WARNING, INFORMATION, MILESTONE, TRACE e VERBOSE.

codefile

Specifica il nome del file di origine del codice dal quale è stato generato il messaggio.

lineum

Specifica il numero della riga nel file di origine del codice in cui è stato generato il messaggio.

msgID

Specifica l'ID assegnato a un evento TNG.

msgDomain

Specifica il nome del dominio dal quale è stato generato il messaggio.

msgNode

Specifica il nome del nodo dal quale è stato generato il messaggio.

msgGenDomain

Specifica il dominio dal quale l'utente identificato dal valore msgGenUser ha generato il messaggio TNG.

msgGenUser

Specifica l'ID dell'utente che ha generato il messaggio TNG.

domainID

Specifica l'ID del dominio dal quale è stato generato il messaggio TNG.

msgDate

Specifica il mese e il giorno (in base all'orologio del sistema) in cui è stato generato il messaggio TNG.

msgTime

Specifica l'ora (in base all'orologio del sistema) in cui è stato generato il messaggio TNG.

eventID

Specifica la stringa evento di origine o l'espressione regolare stile sed che ha attivato l'evento.

arg

Specifica una variabile immessa nella stringa di testo di un'azione di messaggio. Ad esempio, se il campo di testo in un'azione di messaggio viene immesso come "ahd.dll AHD_Call help me", l'argomento in stdlog.0 appare come "args=help me".

tag

Specifica i dati dei tag associati al messaggio TNG.

IPaddr

Specifica l'indirizzo IP dell'host che ha generato il messaggio TNG.

filter

Specifica il nome del processo per il file delle regole di filtro.

filterNum

Specifica il numero del file delle regole di filtro.

majorSrc

Specifica l'origine principale (o il tipo di converter). Si tratta di una stringa che identifica l'ID applicazione di origine. Ovvero, se gli eventi sono originati da Unicenter TNG per Windows (in questo caso il valore è tng), da Unicenter per UNIX (in questo caso il valore è uni) o da un daemon interno (in questo caso il valore è -).

msgScr

Specifica l'origine del messaggio. I valori possibili sono CNV (converter), FLT (filtro), NOS (nessuna origine) e WRT (writer).

msgType

Specifica il tipo di messaggio. I valori possibili sono CRT (creazione), DSC (rilevamento), TRM (interruzione) e UPD (aggiornamento).

msgSrcNum

Specifica il numero dell'origine del messaggio.

platform

Specifica l'ambiente operativo dal quale è stato generato il messaggio. I valori possibili sono AIX, AS400, DECOSF1, DGUX, DYNIX, HPUX, IRIX, MISERVER, MPRAS, MVS, NETWARE, SINIX, SOLARIS, SVR4MP, TANDEM, UNIXWARE, WNT (Windows) o qualsiasi valore definito dagli agenti UNIX.

Caricamento di regole del writer degli eventi

Quando si modificano o definiscono le regole dei writer, è possibile caricarle senza riavviare il server CA Service Desk Manager o uno dei processi di supporto, ad esempio il converter CA NSM o i daemon dei writer e dei filtri. È anche possibile utilizzare questa utilità per scrivere le regole dei writer esistenti in un file.

Per caricare le regole del writer degli eventi, utilizzare l'utilità wrtrule.

Sintassi (caricamento del regole dei writer degli eventi)

La sintassi per il caricamento delle regole dei writer degli eventi è la seguente:

```
wrtrule [-v] [-c addr] [-r rule_file] [-d dump_file]
```


Parametri (caricamento del regole dei writer degli eventi)

-v

Specifica la modalità dettagliata, in modo che vengano visualizzati i commenti durante l'esecuzione dell'utilità.

-c addr

Il nome del writer degli eventi come indicato da `slstat`.

-r rule_file

Il nome del file di testo contenente gli eventi da caricare.

-d dump_file

Il nome del file in cui si desidera scrivere le regole dei writer degli eventi correnti. Nel file vengono scritte i seguenti tipi di informazioni:

- Messaggi di evento in sospeso
- Informazioni delle risorse di rete quando vengono recuperate
- Regole dei writer degli eventi

Nota: sebbene sia facoltativo impostare entrambi i parametri `-r rule_file` e `-d dump_file`, è necessario specificarne almeno uno. È possibile specificarli entrambi, ma in questo caso vengono caricate prima le nuove regole.

Nota: se il writer degli eventi gestisce uno o più messaggi di evento CA NSM quando riceve una richiesta per caricare nuove regole dei writer, il caricamento viene ritardato finché il writer non completa i messaggi correnti. Ad esempio, è possibile che il writer stia elaborando un evento poiché è in attesa delle informazioni relative alle risorse (asset) di rete. In questo caso, il caricamento del messaggio viene ritardato finché non sono state recuperate queste informazioni e non è stata generata una richiesta di chiamata CA Service Desk Manager.

Tuttavia, la richiesta per scrivere le regole degli eventi correnti in un file viene eseguita senza ritardo.

Gestione degli eventi filtrati

Le relazioni tra i daemon dei writer degli eventi e dei filtri e le origini degli eventi su computer diversi vengono gestite nel file della topologia `topology.cfg`, che si trova nella directory `$NX_ROOT/site/eh` (UNIX) o nella directory `directory-installazione\site\eh` (Windows) sul server CA Service Desk Manager. Il file della topologia consente di determinare e gestire l'intero sistema di gestione degli eventi da un'unica ubicazione. Anziché doversi spostare su più client, è possibile modificare i file da un'unica ubicazione e determinare la topologia dell'intero sistema di gestione degli eventi.

Nota: la directory `$NX_ROOT/site/eh` (UNIX) o `directory-installazione\site\eh` (Windows) sul server CA Service Desk Manager include anche le regole dei writer degli eventi e dei filtri.

Utilizzare un editor di testo per visualizzare, aggiornare e salvare il file `topology.cfg`. Si consiglia WordPad per gli utenti Windows e vi per gli utenti UNIX. Non utilizzare un editor di testo che lascia caratteri di formattazione nel file.

Il formato del file della topologia è il seguente:

```
name cmd [dest-name] [converter-type]
```

dove:

nome

Specifica l'host e il nome univoco del daemon di gestione degli eventi nel formato `nomehost:nome-daemon` (ad esempio, `ws2:uconv`). Il `nome-daemon` appare in `s1stat`.

cmd

Specifica il nome dell'eseguibile nella directory `$NX_ROOT/bin` (UNIX) o nella directory `directory-installazione\bin` (Windows), ad esempio `tngcnv`, `uniconvert`, `filter_nxd` o `ehwriter`.

dest-name

Specifica il daemon che riceve gli eventi generici da questo daemon (ad esempio, ws2:filter1 e ws3:wrtr). I daemon dei writer degli eventi non hanno daemon di destinazione. Tutti i daemon devono avere anche un record nel file della topologia.

converter-type

Specifica se gli eventi sono originati da CA NSM per Windows (tng), CA NSM per UNIX (uni) o da un daemon interno (-).

Di seguito è riportato un file della topologia di esempio:

```
# maple:uniconv uniconvert maple:tngfilter uni
maple:tngcnv tngcnv maple:tngfilter tng
maple:tngfilter filter_nxd maple:tngwriter -
maple:tngwriter ehwriter -
```

Esempio

Segue un esempio di come un'organizzazione ha implementato eventi filtrati in un'installazione integrata di CA Service Desk Manager e CA NSM.

Per creare automaticamente delle richieste quando appare lo stato Critico nella mappa CA NSM WorldView, l'amministratore di CA Service Desk Manager (Ken) deve creare una regola di filtro degli eventi per identificare gli eventi a cui desidera rispondere. Deve inoltre creare una regola del writer degli eventi per specificare l'azione da eseguire quando vengono ricevuti eventi di questo tipo.

Ken decide di utilizzare inizialmente una semplice regola di filtro. Quindi, man mano che acquisirà familiarità con il sistema, utilizzerà una serie più complessa di regole. Decide di catturare ciascun evento critico dai server ubicati negli Stati Uniti. Il suo sistema utilizza la convenzione di denominazione per la quale tutti i server ubicati in paesi contigui degli Stati Uniti vengono denominati Usaxxx; ovviamente, si tratta di un metodo molto semplice.

In primo luogo, Ken modifica il file delle regole di filtro tngfilter_rule.datfilter nella directory \$NX_ROOT/site/eh/IP sul server CA Service Desk Manager, dove IP è l'indirizzo IP del server CA Service Desk Manager. Utilizza l'editor UNIX vi, nonostante abbia la possibilità di usare qualsiasi editor di testo che non aggiunge caratteri di controllo estranei (si consiglia agli utenti Windows di utilizzare WordPad per modificare i file).

Nel file `tngfilter_rule.dat`, il segno di cancelletto (`#`) è il carattere dei commenti. Qualsiasi carattere dopo il segno di cancelletto viene ignorato durante la lettura delle regole. La maggior parte delle righe nel file `tngfilter_rule.dat` di Ken sono impostate come commenti, ma Ken osserva le righe seguenti:

```
# Report All Events (separately)
uni:*:*:*:*:(0,1)
tng:*:*:*:*:(0,1)
```

Queste righe costituiscono un filtro aperto; ovvero, un filtro che fa passare tutti gli eventi al writer degli eventi.

Ken modifica queste righe in:

```
# Report All Events (separately)
# uni:*:*:*:*:(0,1)
tng:*:*:*:*:Object_Status_Updated.*Critical.*:(0,1)
```

Ken imposta come commento la riga `uni` poiché al momento è interessato solo agli eventi CA NSM su Windows. Specifica `Object_Status_Updated.*Critical.*` nel campo `event_ID` nella riga `tng` poiché desidera che il filtro faccia passare solo gli eventi `Object_Status_Updated.*Critical.*`. CA NSM genera gli eventi `Object_Status_Updated.*Critical.*` quando lo stato impostato per un oggetto è Critico.

Dopo aver salvato il file delle regole di filtro, Ken modifica il file delle regole dei writer `tngwriter_rule.dat` nella directory `$NX_ROOT/site/eh/IP` sul server CA Service Desk Manager, dove IP è l'indirizzo IP del server CA Service Desk Manager.

Come con le regole di filtro, anche in questo caso la maggior parte delle righe nel file sono commenti. Le ultime due righe nel file mostrano le definizioni delle regole dei writer predefinite. Poiché desidera prendere in considerazione solo gli eventi originati da CA NSM su Windows, Ken imposta come commenti le prime due righe.

Ken specifica il formato della seconda riga attenendosi alla procedura seguente:

1. Ha già impostato il filtro affinché faccia passare solo gli eventi critici; quindi, lascia l'ID evento aperto con .*.
2. Desidera accettare solo gli eventi dai server ubicati negli Stati Uniti; quindi, immette usa.* nel campo del dispositivo.
3. Desidera accettare gli eventi da qualsiasi utente; quindi, il campo dell'utente resta impostato con l'asterisco (*).
4. Desidera scrivere una nuova richiesta per ciascun evento critico; quindi, lascia CR_CREATE nel campo dell'azione.
5. Ha già specificato un modello di richiesta appropriato nel sistema; quindi, ne immette il nome, CriticalTemplate, nel campo del modello.
6. Non desidera che venga eseguita alcuna registrazione; quindi, il campo della registrazione resta impostato su NONE.

I risultati della modifica apportata da Ken sono i seguenti:

```
# .*:*:*:*:uni:*:*:CR_CREATE:::::NONE
*:*:usa.*:*:*:ing:*:*:CR_CREATE::CriticalTemplate:::::NONE
```

Ken salva automaticamente il file delle regole dei writer e riavvia il server CA Service Desk Manager. È pronto per ricevere eventi e scrivere richieste automaticamente.

Risoluzione degli errori di integrazione

Possono verificarsi errori durante l'integrazione, la configurazione e l'utilizzo di CA NSM con CA Service Desk Manager. È possibile risolvere tali errori servendosi delle informazioni seguenti:

- [Messaggi di errore relativi alla mappa 2D/3D \(solo Windows\)](#) (a pagina 558)
- [Analisi della configurazione del server](#) (a pagina 559)
- [Messaggio di errore relativi ai filtri](#) (a pagina 560)
- [Controlla connessione slump](#) (a pagina 562)
- [Attiva registrazione](#) (a pagina 562)

Messaggi di errore relativi alla mappa 2D/3D (solo Windows)

L'integrazione della mappa 2D/3D e di Unicenter Explorer può produrre errori di CA NSM.

TNGWV object create failure= x

Motivo:

Questo errore generalmente si verifica se si esegue più volte lo script di integrazione senza eseguire prima la deintegrazione (x rappresenta un numero).

Azione:

Per deintegrare, e successivamente integrare, CA Service Desk Manager con la mappa 2D/3D di CA NSM e Unicenter Explorer, completare i seguenti passaggi:

1. Nella riga di comando, immettere:
`installation-directory\bin\deintahd.exe`
2. Aprire il browser degli oggetti CA NSM. Selezionare Metodo per visualizzare un elenco di metodi.
3. Se sono presenti dei metodi AHD nella colonna del nome, selezionare Elimina dal menu Oggetto per rimuoverli.
4. Fare clic su Popup_Menu per visualizzare un elenco di menu.
5. Se sono presenti oggetti gestiti da AHD nella colonna del nome, selezionare Elimina dal menu Oggetto per rimuoverli.
6. Con Popup_Menu aperto, scorrere verso il basso finché non viene visualizzata la voce Oggetti gestiti nella colonna del nome.
7. Cercare qualsiasi oggetto gestito il cui nome di metodo contenga AHD. Se vi sono oggetti di questo tipo, selezionare Elimina dal menu Oggetto per rimuoverli.
8. Fare clic sulla voce Jasmine_Menu_Action per visualizzare un elenco di metodi di Unicenter Explorer. Se sono presenti azioni di menu USPSD nella colonna del nome, selezionare Elimina dal menu Oggetto per rimuoverle.

9. Fare clic sulla voce Jasmine_Menu_Object per visualizzare un elenco di menu di Unicenter Explorer. Se sono presenti oggetti menu USPSD nella colonna del nome, selezionare Elimina dal menu Oggetto per rimuoverli.
10. Chiudere il browser degli oggetti.
11. Nella riga di comando, immettere:

`installation-directory\bin\integAHD.exe`

A questo punto, l'integrazione delle mappe 2D/3D e di Unicenter Explorer dovrebbe essere completa. Fare clic con il pulsante destro del mouse su un oggetto gestito a partire dalla mappa 2D/3D o da Unicenter Explorer e verificare che tutte le opzioni di menu di CA Service Desk Manager siano visualizzate.

CAE0232E-Repository error code 22

Motivo:

Questo messaggio indica che il percorso per l'eseguibile nell'elenco Metodo non è corretto.

Azione:

Aggiungere directory-installazione\bin al percorso oppure modificare il campo exe_name nell'elenco Metodo per includere il percorso completo dell'eseguibile.

Analisi della configurazione del server

Quando il server CA Service Desk Manager si trova su un computer UNIX o Windows e CA NSM è installato in un altro computer Windows, è necessario che il server CA Service Desk Manager sia attivo e in esecuzione. Avviare il servizio NSM Event Converter sul computer CA NSM. Per verificare che il convertitore sia attivo e in esecuzione, controllare i processi utilizzando Task Manager. Se tngcnv non viene visualizzato come processo in esecuzione dopo l'avvio del servizio Event Converter, verificare gli ultimi file tngcnv.*n* o stdlog.*n* (disponibili in *directory-installazione\log*). Questi file illustrano i motivi della mancata esecuzione del convertitore di eventi.

Quando il server CA Service Desk Manager e il server CA NSM si trovano sullo stesso computer Windows, il servizio CA Service Desk Manager deve essere attivo e in esecuzione. Avviare il servizio CA NSM Event Converter sul computer. Per verificare che il convertitore sia attivo e in esecuzione, controllare i processi utilizzando Task Manager. Se tngcnv non appare come processo in esecuzione dopo l'avvio del servizio CA Service Desk Manager, verificare quanto segue:

1. Utilizzando WordPad, modificare il file pdm_startup riportato nella *directory- installazione*\pdmconf. In questo file, viene visualizzato un testo simile al seguente:

```
[procset MAIN_PROCSET]
pdm_info
sw_ver_ctl
bpnotify_nxd
PDMBASE
PDMBOP
FILTERING
```

Se è utilizzato un punto e virgola (;) per impostare FILTERING come commento, rimuovere tale carattere.

2. Quando ci sposta verso l'alto per tornare all'inizio del file, dovrebbe essere visualizzato il testo seguente:

```
[procset FILTERING]
tngfilter
tngwriter
ehc
; UNICNV_REPLACE
; tngcnv:NT_ONLY
```

Se è utilizzato un punto e virgola (;) per impostare una delle precedenti opzioni come commento, rimuovere tale carattere.

3. Se si apportano modifiche a questo file, salvarle e riavviare il server CA Service Desk Manager.

Se il convertitore di eventi non viene ancora visualizzato come processo in esecuzione, controllare il file *tngcnv.n* più recente (che si trova in *directory- installazione*\log). Questo file illustra il motivo della mancata esecuzione del convertitore di eventi.

Messaggi di errore relativi ai filtri

Se il converter eventi (tngcnv) non è avviato oppure è in esecuzione ma non viene creata alcuna richiesta, i file di registro possono contenere un errore indicante il motivo per il quale il converter non è stato avviato o non ha potuto riportare gli eventi. È possibile che venga visualizzato uno o più dei seguenti messaggi di errore:

Impossibile risolvere il nome host in un indirizzo IP

Motivo:

Questo messaggio indica che mancano le voci host sul computer CA Service Desk Manager, CA NSM o su entrambi i computer.

Questo errore può indicare anche che DNS non è in funzione o non restituisce l'indirizzo IP corretto.

Azione:

Controllare il file %SystemRoot%/system32/drivers/etc/hosts. Il file host deve contenere una voce per i computer CA Service Desk Manager e CA NSM. Dopo l'aggiunta del nome host, riavviare il converter (o il servizio CA Service Desk Manager). Di seguito è riportato un esempio:

```
127.0.0.1    localhost    # Local host loop back
141.202.211.11  usbegp11    # This is the NSM client box
141.202.211.12  usbegp12 ahdhost # This is the Service Desk host
                # (showing multiple entries)
```

Impossibile trovare il file del repository

Motivo:

Questo messaggio indica che il parametro @NX_REPOSITORY non è impostato nel file NX.env (che si trova nella directory *directory-installazione*) sul client.

Azione:

Modificare NX.env, aggiungere il nome del repository specificandolo con attenzione, salvare il file e riavviare il converter eventi.

La dipendenza non esiste o è stata contrassegnata per l'eliminazione

Motivo:

Questo messaggio viene visualizzato quando sul convertitore viene rilevata una dipendenza (probabilmente MSSQL) che deve essere rimossa.

Azione:

Eseguire regedt32 e aprire la struttura HKEY_LOCAL_MACHINE -> System -> Current Control Set -> Services -> AHD_Event_Converter. Rimuovere la dipendenza MSSQL (o qualsiasi altra dipendenza) e riavviare il server Windows.

"Destinazione sconosciuta. Eventi in coda." o "Nessuna voce del file topology.cfg per il nodo. Evento in coda."

Motivo:

Questo messaggio indica che è necessario correggere il file topology.cfg sul server CA Service Desk Manager.

Azione:

Correggere il file topology.cfg come necessario, quindi riavviare CA Service Desk Manager e il converter CA NSM. Di seguito è riportato un esempio di un file topology.cfg per CA Service Desk Manager su un computer Windows denominato AHD1 e su un computer CA NSM denominato TNG:

```
TNG1:tngcnv tngcnv AHD1:tngfilter tng
AHD1:tngfilter filter_nxd AHD1:tngwriter -
AHD1:tngwriter ehwriter -
```

Modalità di verifica della connessione slump

Se il convertitore CA NSM è in esecuzione e ancora non viene creato alcun evento, controllare la connessione slump a CA Service Desk Manager.

Per controllare la connessione, effettuare le operazioni seguenti:

1. Utilizzare il comando *s/stat* dalla riga di comando nel computer su cui è in esecuzione CA Service Desk Manager.
2. Cercare una connessione a tngcnv.
Se non ne viene trovata nessuna, il converter non comunica con CA Service Desk Manager.
3. Riavviare il convertitore CA NSM, quindi controllare nuovamente la connessione.
4. Se ancora non è possibile trovare la connessione, controllare i file tngcnv.n (che si trovano in *directory-installazione\log*) per ricercare gli errori relativi all'accesso a slump e tngcnv.

Attiva registrazione

Se l'accesso a slump è riuscito e ancora non vengono visualizzati nuovi eventi, attivare la registrazione e controllare i file per ricercare l'indicazione che un evento è stato trasferito a CA NSM. È possibile creare un evento semplicemente modificando lo stato su un oggetto gestito nella mappa 2D/3D.

Per attivare la registrazione, modificare il file NX.env che si trova nella directory \$NX_ROOT (UNIX) o nella directory *directory-installazione* (Windows) per includere la riga seguente:

```
@NX_LOG_LEVEL_BSTRAP=VERBOSE
```

È possibile monitorare i file `tngcnv.n` (che si trovano nella directory *directory-installazione\log*) per determinare se gli eventi vengono trasferiti a CA Service Desk Manager. Dovrebbe essere visualizzato un testo simile al seguente:

```
09/17 16:35:58:01 tngcnv 477 MILESTONE convtr.c 399
Sending 1:::dogwood:::9994011e-2f7e-11d1-a435-00c04fd478c9:::09/17/1997
:::16:35:41:::Object_Status_Updated minor:::BV:141.202.211.0:Segment.1
IP:141.202.211.14 MAC: CNT: LOC: DSC:::3:::tngcnv:1:::tng:::WindowsNT:
:::CNV:::CRT:::1:::
```

In questo esempio, il messaggio indica che lo stato per un oggetto gestito è stato aggiornato a Meno importante.

Se gli eventi vengono trasferiti a CA Service Desk Manager e appaiono nel registro, eseguire un doppio controllo per verificare che siano utilizzate le regole predefinite dei writer e dei filtri. In caso contrario, ripristinare i file dei writer e dei filtri originali, riavviare il server e creare un nuovo evento.

Se gli eventi non vengono trasferiti a CA Service Desk Manager, accertarsi che siano in esecuzione due processi di CA NSM responsabili del trasferimento delle informazioni relative agli eventi (`canotify.exe` e `caoprdsn.exe`). Se non sono in esecuzione, avviarli come descritto nella documentazione relativa a CA NSM. Se sono in esecuzione, rivolgersi al supporto di CA NSM.

CA Service Desk Manager Event Converter

Queste informazioni si applicano solo all'integrazione di CA NSM in un ambiente operativo Windows.

CA Service Desk Manager Event Converter viene installato in due diversi modi quando la configurazione CA Service Desk Manager è in esecuzione su un server Windows:

- Si installa come servizio Windows
- Si installa come parte del servizio CA Service Desk Manager Daemon Server dal quale è possibile avviare e interrompere l'esecuzione del convertitore.

È possibile eseguire Event Converter su un computer primario, secondario o solo client. È possibile avviare il convertitore sui server primario e secondario utilizzando entrambi i metodi, mentre è possibile avviarlo su un client solo come servizio Windows.

Nota: se CA Service Desk Manager viene arrestato, è possibile lasciare Event Converter in esecuzione per consentire la ricezione di messaggi da NSM. Tutti i messaggi ricevuti da NSM mentre CA Service Desk Manager non è attivo vengono messi in coda ed elaborati nel momento in cui CA Service Desk Manager viene riavviato.

Rimozione del convertitore eventi (Gestore daemon)

Gestore daemon avvia e interrompe l'esecuzione del convertitore e consente inoltre di riavviarlo se viene arrestato involontariamente. È possibile utilizzare *pdm_status* per scoprire se il convertitore è in esecuzione o meno e determinare se è in esecuzione sul server locale o su un server remoto (secondario).

Se si desidera utilizzare Gestore servizio Windows per avviare e interrompere il convertitore eventi, rimuoverlo dalla configurazione di avvio di Gestore daemon.

È possibile modificare la configurazione di avvio su un server primario modificando la riga *tngcnv* nel file *pdm_startup* in modo che riporti quanto segue:

```
; tngcnv.
```

Importante Questa modifica viene annullata se si esegue di nuovo la configurazione di CA Service Desk Manager. Se si desidera mantenere la modifica dopo aver eseguito la configurazione, modificare *pdm_startup.tpl*.

Per modificare la configurazione di avvio su un server remoto (secondario), utilizzare la funzionalità *pdm_edit*.

Nota: per ulteriori informazioni sull'esecuzione di *pdm_edit*, consultare la *Guida all'amministrazione*.

Rimozione del convertitore eventi (servizio Windows)

Se si desidera utilizzare Gestore daemon per avviare e interrompere l'esecuzione del convertitore eventi, utilizzare il comando seguente per rimuovere il convertitore eventi dal servizio Windows:

```
tngcnv -u
```

È possibile reinstallare il convertitore eventi come servizio Windows utilizzando il comando seguente:

```
tngcnv -i
```

Potenziamento del processo di integrazione di NSM a CA Service Desk Manager

In questa sezione viene fornito un esempio di come usufruire dell'integrazione tra CA NSM e CA Service Desk Manager. L'esempio descrive un metodo semplice per configurare questa funzionalità predefinita, ma non deve essere considerato come l'unico metodo disponibile per eseguire questa attività.

Record/azioni dei messaggi di esempio con contenuto limitato

Due record messaggio, CFNEW e CFUPDATE, scritti con una singola azione di messaggio ciascuno, rappresentano il fondamento in questo esempio per l'integrazione di NSM a CA Service Desk Manager (sono inclusi anche file di esempio). Per un'integrazione pulita, compatta, solida e di facile gestione, è possibile avvalersi dei seguenti elementi:

- tngwriter_rule.dat
- funzioni CR_UPDATE e CR_UPDATE_ONLY
- elenco parole chiave text_api

Nota: l'esempio mostra come creare record messaggio e azioni dei messaggi con contenuto molto limitato. Il contenuto è stato spostato nei comandi cawto descritti negli esempi che seguono. In alternativa, è possibile inserire i parametri e il contenuto desiderati direttamente nel campo "testo" dell'azione di messaggio oppure utilizzare una combinazione dei due metodi.

Esempio di record messaggio di Gestione eventi

Quando si utilizza questa integrazione, è possibile utilizzare la pagina dei dettagli del record messaggio per visualizzare un esempio di record messaggio di Gestione eventi che reagirà a un evento contenente "CFNEW" all'inizio dell'avviso di evento.

Esempio di elenco di azioni dei messaggi

Quando si usufruisce di questa integrazione, è possibile utilizzare l'elenco di azioni dei messaggi associato al record messaggio "CFNEW*". Facendo doppio clic su questa voce, vengono visualizzate informazioni dettagliate archiviate come parte dell'azione messaggio. Se si continua a utilizzare l'integrazione, è possibile visualizzare una vista dettagliata con il campo "action" impostato su "EXTERNAL" e il campo "text" con il valore di testo di integrazione standard "AHD.dll AHD_Call".

Esempio di record messaggio (configurato per cercare eventi che iniziano con CFUPDATE)

Quando si usufruisce di questa integrazione, è possibile utilizzare le informazioni dettagliate restituite da un secondo record messaggio, configurato per cercare eventi che iniziano con "CFUPDATE". Anche per questo record messaggio è stata creata un'identica azione messaggio (come mostrato nel precedente record messaggio "CFNEW*"):

Esempio di comandi cawto per la creazione e l'aggiornamento delle richieste

Per utilizzare i record messaggio creati in precedenza, inviare un messaggio tramite la funzione Gestione eventi di CA NSM utilizzando il comando/utilità "cawto" disponibile in CA NSM. Il comando/l'utilità "cawto" consente di creare o aggiornare una richiesta utilizzando i formati dei comandi riportati negli esempi che seguono.

Nota: utilizzando questo metodo, è possibile catturare e riformattare (per la conversione in un formato supportato in CA Service Desk Manager) i messaggi di avvertenza desiderati generati dalla console di Gestione eventi.

Eseguire il comando "opreload" sulla console di Gestione eventi NSM per aggiornare le azioni e i record messaggio di evento NSM memorizzati dopo la creazione delle regole precedenti relative alle azioni e ai messaggi NSM.

Esempio 1: formati "cawto" per la creazione e l'aggiornamento di una nuova richiesta

Utilizzare il seguente formato cawto per la creazione di una nuova richiesta:

```
CAWTO -n <nome-server-NSM>  
CFNEW;%STRING1=KEYWORD1;%CUSTOMER=ServiceDesk;%SUMMARY=Photos  
required;%CATEGORY=Applications;%DESCRIPTION=Description: Photos required Justification: required  
by regulations for entry
```

Utilizzare il seguente formato cawto per l'aggiornamento di una nuova richiesta:

```
CAWTO -n <nome server-NSM>  
CFUPDATE;%STRING1=KEYWORD1;%STATUS=Closed;%SUMMARY=Cancelled by ServiceDesk
```

Esempio 2: formati "cawto" alternativi per la creazione e l'aggiornamento di una nuova richiesta

Utilizzare il seguente formato cawto alternativo per la creazione di una nuova richiesta:

```
CAWTO -n <nome-server-NSM> CFNEW2;%EVENT_TOKEN=KEYWORD2;%SUMMARY=Server  
Installation Approved;%STATUS=Work in Progress;%CATEGORY=Hardware;%DESCRIPTION=Install  
new server and level V drops to existing server location within the data center. Also, install wiring on patch  
panel in router cabinet
```

Utilizzare il seguente formato cawto alternativo per l'aggiornamento di una nuova richiesta:

```
CAWTO -n <nome-server-NSM>  
CFUPDATE2;%EVENT_TOKEN=KEYWORD2;%STATUS=Closed;%SUMMARY=Closed by Server  
Team
```

File di esempio da utilizzare con l'integrazione

Quando NSM viene integrato in CA Service Desk Manager è possibile utilizzare alcuni file di esempio.

topology.cfg

```
# <remote_node>:uniconv uniconvert <IP_ADDR_tngfilter>:tngfilter uni
<IP_ADDR_tngcnv>:tngcnv tngcnv <IP_ADDR_tngfilter>:tngfilter tng
<IP_ADDR_tngfilter>:tngfilter filter_nxd <IP_ADDR_tngwriter>:tngwriter -
<IP_ADDR_tngwriter>:tngwriter ehwriter - -
```

dove:

<IP_ADDR_tngcnv>

L'indirizzo IP del server che esegue il processo del convertitore eventi CA NSM.

<IP_ADDR_tngfilter>

L'indirizzo IP del server che esegue CA Service Desk Manager.

<IP_ADDR_tngwriter>

L'indirizzo IP del server che esegue CA Service Desk Manager.

tngfilter_rule.dat

Utilizzare la versione predefinita di questo file, senza apportare modifiche.

tngwriter_rule.dat

Il file tngwriter_rule.dat viene visualizzato nel modo seguente:

```
# evt
id::dev::user::majorSrc::minorSrc::action::template::cmd::log::event_token::user_parms
```

dove:

event id

La stringa o l'espressione regolare stile sed.

device

La stringa, l'espressione regolare stile sed, '*' o nessun valore.

utente

La stringa, '*' o nessun valore.

majorSrc

La stringa "uni" da uniconverter o "tng" da tng converter.

minorSrc

La stringa o '*'.

azione

Le opzioni di azione. Sono disponibili le opzioni seguenti:

CR_CREATE

Consente di scrivere una nuova richiesta per ciascun evento.

CR_UPDATE

Consente di aggiornare una o più richieste oppure di creare una nuova richiesta se non vi sono richieste esistenti. Per impostazione predefinita, le richieste vengono localizzate tramite la corrispondenza dei campi (asset) log_agent e affected_resource. È possibile ignorare i valori predefiniti specificando un elenco di attributi di richiesta di chiamata.

CR_UPDATE_ONLY

Consente di eseguire le operazioni di CR_UPDATE, ma non viene creata alcuna nuova richiesta quando non vengono trovate richieste corrispondenti.

COMMAND

Esegue <cmd>, identificato nella descrizione cmd in questa tabella.

modello

Specifica il nome del modello da utilizzare per creare una richiesta. Questo parametro non è obbligatorio e viene ignorato se l'azione è diversa da CR_CREATE.

Nota: è necessario creare il modello di richiesta prima della definizione della regola.

cmd

Il comando comunicato alla shell, ignorato in tutte le azioni tranne nell'azione COMMAND.

registrazione

Le opzioni di registrazione, indicate dai seguenti valori:

NESSUNO

Nessuna registrazione (tranne la registrazione degli errori).

SYS

Registrazione degli incidenti nel syslog UNIX (console dei messaggi Unicenter).

PDM

Registrazione degli incidenti nel registro delle applicazioni (\$NX_ROOT/log).

BOTH

Registrazione degli incidenti nel syslog e nel registro delle applicazioni.

event_token

(Facoltativo). Tag di 30 caratteri definito dall'utente che identifica una specifica richiesta associata a un event_id (messaggio di evento tng) o tutti i messaggi come un event_id (ad esempio, un event_id con caratteri jolly).

Il parametro event_token è un attributo di richiesta memorizzato in ogni richiesta generata dall'interfaccia di TNG. Se non è specificato alcun event_token nella regola del writer, viene utilizzata la stringa "tng_generated". Ciò consente di aggiornare tutte le richieste che corrispondono all'attributo event_token. Ad esempio, due diversi messaggi per lo stesso asset possono aggiornare richieste univoche. Ciascuna regola del writer CR_UPDATE specifica le parti univoche del messaggio e un event_token univoco. L'event_token viene utilizzato per ricercare e aggiornare la richiesta corrispondente. Per impostazione predefinita, un registro di attività contenente il messaggio viene aggiunto alla richiesta corrispondente.

In un altro esempio, è possibile aggiornare l'attributo dello stato (ad esempio, impostare stato=CL (chiuso)) in una richiesta esistente specificando lo stesso event_token nella regola del writer CR_UPDATE utilizzata quando la richiesta è stata creata con una regola del writer CR_CREATE.

user_parms

(Facoltativo) Contiene i tre tipi di dati seguenti:

- Valori attributi richiesta
- Un elenco degli attributi di richiesta per la corrispondenza durante l'aggiornamento dei record richiesta esistenti
- Nomi di parametri speciali sostituiti da valore corrispondente proveniente dalla struttura di eventi TNG

I valori di richiesta e l'elenco di attributi vengono specificati mediante la sintassi %<KEYWORD>=<value>. Se si utilizzano più coppie parola chiave/valore, separarle inserendo un carattere di punto e virgola (";").

I valori degli attributi di richiesta vengono specificati utilizzando la sintassi %<ATTRIBUTE>=<value>, dove ATTRIBUTE corrisponde al nome di un attributo identificato nel file text_api.cfg (che si trova nella directory \$NX_ROOT/site), associato a un attributo di richiesta AHD majic.

La sintassi per l'elenco di attributi per la corrispondenza viene specificata come %SEARCH=<attribute1>[,<attribute2>...], dove SEARCH è una parola chiave fissa e attribute1, attribute2 e così via sono nomi di ATTRIBUTO specificati nel file text_api.cfg.

È possibile utilizzare i seguenti nomi di parametri speciali nella stringa user_parms:

&Message

Il testo associato al messaggio CA NSM.

&Parm

Il campo Parm AHD.DLL della finestra di dialogo Azione messaggio di CA NSM.

&Uuid

L'identificativo univoco universale di TNG.

&Device

Il dispositivo, ad esempio il nome host, che ha generato il messaggio CA NSM.

&Majorsrc

Il tipo di origine principale che indirizza gli eventi al writer degli eventi. Per gli eventi provenienti da CA NSM su Windows, il valore è "tng". Per gli eventi provenienti da CA NSM su UNIX, il valore è "uni".

&Minorsrc

Il tipo di origine secondario che indirizza gli eventi al writer degli eventi.

&Node

Il dispositivo (ad esempio, il nome host) che ha generato il messaggio CA NSM.

&Addr

L'indirizzo IP dell'host che ha generato il messaggio CA NSM.

&Username

Il nome utente sull'host che ha generato il messaggio CA NSM.

&Date

Un numero intero che indica quando è stato generato il messaggio CA NSM, a partire dal 1970.

&Time

La data e l'ora del messaggio CA NSM. Ad esempio, Mar 4 luglio 10:23:37 2000.

&Severity

La gravità del messaggio CA NSM.

&Tag

I dati dei tag associati al messaggio CA NSM.

Come esempio, se si utilizzano gli esempi riportati in Esempio 2: formati "Cawto" alternativi per la creazione e l'aggiornamento di una nuova richiesta, il file predefinito delle regole del writer degli eventi dovrebbe essere modificato da:

```
*...*...:uni:...:CR_CREATE:.....:NONE
```

a:

```
CFNEW.*...*...:tng:...:CR_UPDATE:.....:NONE:.....&Parm;%SEARCH_EXPLICIT=STRING1
CFNEW2.*...*...:tng:...:CR_UPDATE:.....:NONE:.....&Parm;%SEARCH=Event_Token
CFUPDATE.*...*...:tng:...:CR_UPDATE_ONLY:.....:NONE:.....&Parm;%SEARCH_EXPLICIT=STRING1
CFUPDATE2.*...*...:tng:...:CR_UPDATE:.....:NONE:.....&Parm;%SEARCH=EVENT_TOKEN;%STATUS=C
L
```

Nota: il parametro %SEARCH_EXPLICIT viene utilizzato per assicurarsi che, al momento di un aggiornamento, la ricerca individui una richiesta corrispondente confrontando il contenuto del campo STRING1 prima di procedere con l'aggiornamento. Per ulteriori informazioni su text_api.cfg e su come CA Service Desk Manager utilizza API testo per generare richieste da CA NSM, consultare la *Guida all'amministrazione*.

Ulteriori informazioni:

[Definizioni delle regole dei writer degli eventi](#) (a pagina 540)

Integrazione di Portale CA

È possibile accedere ai componenti di CA Service Desk Manager mediante CA Management Portal e Portale CA.

Nota: CA Management Portal e Portale CA non sono inclusi in CA Service Desk Manager ed è necessario acquistarli e acquisirne la licenza separatamente. In CA Service Desk Manager sono contenute solo le informazioni di base per accedere a CA Service Desk Manager tramite Portal Administration. Per informazioni dettagliate, consultare la *Guida in linea di CA Management Portal Server Administration* e Portale CA.

Verifica dell'accessibilità dell'interfaccia Web di CA Service Desk Manager

Dopo aver installato CA Service Desk Manager in un sistema, assicurarsi di poter accedere all'interfaccia Web tramite il server Tomcat. Per consentire il corretto funzionamento dell'integrazione del portale, è necessario che l'interfaccia Web di CA Service Desk Manager sia accessibile tramite Tomcat.

Nota: per l'installazione del server LINUX di CA Service Desk Manager, è necessario impostare LD_LIBRARY_PATH su \$NX_ROOT/sdk/lib.

Installazione e avvio di Portale CA

Per informazioni dettagliate sull'installazione, l'avvio e l'arresto di Portale CA, consultare la *Guida introduttiva di Portale CA* valida per la propria installazione.

Nota: è possibile installare Portale CA sullo stesso sistema in cui è installato CA Service Desk Manager o su un sistema diverso.

Inclusione dei portlet

È possibile utilizzare il prodotto per includere i portlet di CA Service Desk Manager nel portale.

Per includere i portlet

1. Accedere a CA Service Desk Manager e fare clic su Ricerca in Gestione opzioni nella scheda Amministrazione.
Viene visualizzata la finestra Elenco opzioni.
2. Fare clic su Portal_Safe_List.
Viene visualizzata la finestra dei dettagli di Portal_Safe_List.
3. Immettere il *servername:portnumber* in cui è stato installato il portale nel campo Valore opzioni.
Nota: per ulteriori informazioni su questa opzione, consultare la *Guida in linea*.
4. Fare clic su Installa.
5. Riavviare il daemon di CA Service Desk Manager.
6. Effettuare l'accesso a Portale CA come amministratore.

7. Creare un utente CA Service Desk Manager valido. Per ulteriori informazioni su come creare un utente, consultare la documentazione relativa a Portale CA.

Nota: la password utilizzata durante la creazione dell'utente nel portale può essere diversa da quella utilizzata dallo stesso utente per accedere a CA Service Desk Manager, in quanto CA Service Desk Manager autentica gli utenti per l'integrazione utilizzando una combinazione di nome utente, sessione Portale CA valida e valore di installazione Portale CA, se esiste nell'opzione PORTAL_SAFE_LIST.

8. Selezionare Conoscenza dalla barra dei menu principale di Portale CA.

Viene visualizzata la pagina Conoscenza.

9. Selezionare Libreria dalla barra Conoscenza del riquadro sinistro.

Viene visualizzata la struttura Libreria nel riquadro di sinistra.

10. Selezionare, oppure creare e selezionare se necessario, una cartella nella struttura Libreria, quindi selezionare Pubblica file sulla barra Conoscenza del riquadro di destra.

Viene visualizzato il modulo Pubblica file.

11. Digitare l'URL del portlet CA Service Desk Manager seguente nella casella di testo Contenuto della scheda Informazioni generali:

```
http://hostname:portnumber/CAisd/PortalServlet?USERNAME=$USER.username$&PORTALSESSION=$SESSION$&PORTALINSTALL=portalhostname:portalportnumber
```

Nota: sostituire *hostname:portnumber* nell'URL con il nome e la porta del server Web in cui si trova CA Service Desk Manager. Sostituire *portalhostname:portalportnumber* nell'URL con il nome e la porta del server Web su cui si trova Portal.

12. Digitare CA Service Desk Manager nella casella di testo Titolo.

13. Fare clic su Avanzate.

Viene visualizzata la pagina delle proprietà avanzate del modulo Pubblica file.

14. Digitare *portal/variable-url* nel campo Tipo di contenuto MIME e fare clic su Pubblica.

Il contenuto pubblicato viene visualizzato nella cartella Libreria selezionata.

15. Configurare l'area di lavoro per la visualizzazione di questo portlet.
16. Scollegarsi e accedere come nuovo utente. L'accesso a CA Service Desk Manager nel portlet appena creato dovrebbe avvenire automaticamente senza doversi ricollegare.

Nota: durante l'esecuzione di CA Service Desk Manager nel portlet, la preferenza Non visualizzare popup non è disponibile nella pagina Preferenze. Indipendentemente dall'impostazione della preferenza viene sempre utilizzata una finestra popup.

Connessione al server Portale CA

Per connettersi al server Portale CA, utilizzare un browser Web e immettere l'URL seguente nel campo della posizione o dell'indirizzo:

`http://<nomeserver>:<n.porta#>/servlet/portal`

<nomeserver>

Specifica il nome (o l'indirizzo IP) del server del portale.

<n.porta>

Specifica il numero di porta monitorato dal server Portale CA. Il numero di porta viene specificato durante l'installazione del server Portale CA. Il valore predefinito è 8080.

Configurazione di CA Service Desk Manager per l'utilizzo di SSL con Portale CA

Nota: ai fini della produzione, è consigliabile ottenere sempre un certificato da un'autorità di certificazione attendibile.

Prima di configurare CA Service Desk Manager per l'utilizzo di SSL, verificare che l'integrazione tra Portale CA e CA Service Desk Manager funzioni senza SSL. Se l'integrazione funziona senza SSL, è possibile includere i portlet.

Ulteriori informazioni:

[Inclusione dei portlet](#) (a pagina 572)

Configurazione di SSL tramite un'autocertificazione

Per configurare l'integrazione del portale CA Service Desk Manager con un'autocertificazione

1. Nella riga di comando, immettere:

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

Rispondere ai prompt nel modo appropriato e immettere "changeit" come password per entrambi i prompt della password.

Viene configurato il certificato.

2. Modificare il file che si trova in:

```
$NX_ROOT/bopcfg/www/CATALINA_BASE/conf
```

3. Rimuovere i commenti della sezione seguente e salvare:

```
<!--
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
  port="8443" minProcessors="5" maxProcessors="75" enableLookups="true" acceptCount="100"
  debug="0" scheme="https" secure="true" useURValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
  clientAuth="false" protocol="TLS" /></Connector>
-->
```

4. Aggiungere l'attributo keystoreFile al file server.xml. Quando si esegue il comando nel passaggio 1, viene creato un file con estensione keystore nella directory principale dell'utente. Aggiungere il riferimento all'attributo keystoreFile e salvare il file. Il file server.xml dovrebbe apparire come indicato di seguito.

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
  port="8443" minProcessors="5" maxProcessors="75" enableLookups="true" acceptCount="100"
  debug="0" scheme="https" secure="true" useURValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
  clientAuth="false" protocol="TLS" keystoreFile="location/.keystore" />
</Connector>
```

5. Riavviare CA Service Desk Manager.
6. Per verificare la funzionalità SSL, immettere nel browser l'indirizzo *https://hostname:8443*. Dovrebbe essere visualizzata la finestra di dialogo Avviso di protezione. Fare clic su Sì.

Nota: SSL utilizza la porta 8443.

7. Sostituire il portlet CA Service Desk Manager per utilizzare HTTPS e la porta 8443.

`https://nomehost:8443/CAisd/PortalServlet?`

`USERNAME=$USER.nomeutente&&PORTALSESSION=$SESSION&&PORTALINSTALL=nomehostportale:numeroportaportale`

Connessione a CA Service Desk Manager quando Portale CA utilizza SSL

È possibile importare il certificato del server Portale CA e stabilire una connessione affidabile tra CA Service Desk Manager e Portale CA (quando quest'ultimo è configurato per utilizzare SSL).

Per connettersi a CA Service Desk Manager quando il portale utilizza SSL

1. Verificare che Portale CA sia configurato e funzioni con SSL.

Nota: per informazioni sul processo di verifica, vedere la documentazione di Portale CA.

2. Esportare il certificato dal computer nel quale è installato Portale CA, attenendosi alla procedura seguente:

- a. Individuare il file `server.xml` nel percorso seguente:

`PORTAL_Install_Dir\jakarta-tomcat-4.1.29\conf.`

- b. Prendere nota della posizione del keystore e della password (`pwd`), come illustrato nelle seguenti righe contenute nel file `server.xml`. La password predefinita è *changeit* (tutto minuscolo). Se è stata utilizzata una password personalizzata per la creazione del certificato durante la configurazione del portale, sarà necessario utilizzare tale password. Per ulteriori informazioni, consultare la documentazione di Portale CA. Nei passaggi ed esempi seguenti la password predefinita utilizzata è *changeit*:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
  port="8443" minProcessors="5" maxProcessors="150"
  enableLookups="true"
  acceptCount="100" debug="0" scheme="https" secure="true"
  useURValidationHack="false" disableUploadTimeout="true">
  <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
    keystoreFile="c:\Programmi\CA\SC\Unicenter Management Portal\UMPkeystore"
    keystorePass="changeit"
    clientAuth="false" protocol="TLS" />
</Connector>
```

- c. Individuare la directory JRE bin (`PORTAL_Install_Dir\jre\bin`) nel server del portale per accedere all'utilità `keytool` che verrà utilizzata per esportare il certificato del server PORTAL in un file.

- d. Accedere all'utilità keytool utilizzando il seguente comando:
`keytool -export -alias tomcat -file umpserver.cer -keystore "c:\Programmi\CAS\Unicenter Management Portal\UMPkeystore"`

Immettere la password keystore: *changeit*

Certificato salvato nel file <umpserver.cer>

Nota: quando viene richiesta la password, occorre utilizzare quella ottenuta al passaggio 2b. Nell'esempio precedente, *changeit* è la password annotata al passaggio 2b. La posizione del keystore viene ottenuta anche al passaggio 2b.

3. Importare il certificato ottenuto dal server nel computer con l'installazione di CA Service Desk Manager, utilizzando l'utilità keytool come segue:

- a. Nel computer con CA Service Desk Manager individuare la directory JRE\bin generalmente disponibile nella posizione seguente:
`C:\Programmi\CAS\JRE\bin.`

- b. Il certificato deve essere importato nell'Autorità di certificazione utilizzata da CA Service Desk Manager Java Virtual Machine.

Di seguito è riportato l'esempio di un'importazione. In questo esempio la posizione dell'Autorità di certificazione è:

`C:\Programmi\CAS\JRE\1.4.2_06\lib\security\cacerts`

Quando viene chiesta una *password*, immettere "changeit". Quando viene chiesto se considerare *attendibile il certificato*, immettere Yes.

`Keytool.exe -import -alias tomcat -trustcacerts -file umpserver.cer -keystore "C:\Programmi\CAS\JRE\1.4.2_06\lib\security\cacerts"`

Immettere la password keystore: *changeit*

Proprietario: CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny, C=us

Rilasciato da: CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny, C=us

Numero di serie: 43ecb469

Valido da: ven feb 10 10:42:33 EST 2006 fino a: gio mag 11 11:42:33 EDT 2006

Certificate fingerprints (Impronta digitale del certificato):

MD5: A1:AF:AE:92:39:2E:53:D5:1C:6D:FE:44:68:61:DD:5C

SHA1: 66:3A:BC:77:32:81:60:89:70:B9:EF:FB:74:3D:93:74:CD:8E:E2:D2

Trust this certificate? (Certificato attendibile?) [no]: yes

Certificate was added to keystore (Certificato aggiunto a keystore)

Nota: quando viene richiesta la password, utilizzare quella ottenuta al passaggio 2b. Nell'esempio precedente, *changeit* è la password annotata al passaggio 2b.

4. Modificare il file portal-xml-api.xml in
`$NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAsd\WEB-INF\xml\portal-xml-api.xml` effettuando le operazioni seguenti:

- a. Sostituire HTTP nella riga:

`<!DOCTYPE PORTAL SYSTEM "http://127.0.0.1:8080/servlet/media/xml/api/request.dtd">`

con HTTPS:

```
<!DOCTYPE PORTAL SYSTEM "https://127.0.0.1:8080/servlet/media/xml/api/request.dtd">
```

- b. Salvare il file.
- c. Se Portal_Safe_List è stato installato, assicurarsi di modificare il numero di porta in 8443 e il nome del computer in modo da includere il nome di dominio, ad esempio machinename.ca.com:8443.

Importante Includere il nome del dominio nel nome del computer poiché il certificato del portale contiene tale nome. Per ulteriori informazioni, consultare la documentazione di Portale CA.

- 5. Riciclare il server CA Service Desk Manager.
- 6. Da Portale CA, effettuare una connessione al portlet CA Service Desk Manager utilizzando il seguente URL:

```
http://hostname:portnumber/CAisd/PortalServlet?USERNAME=$USER.username$&PORTALSESSION=$SESSION$&PORTALINSTALL=servername:8443
```

Nota: sostituire *servername* nell'URL con il nome del server Web su cui si trova Portale CA. Il nome del server in questo URL deve includere il nome del dominio, ad esempio, servername.ca.com:8443. Sostituire hostname:portnumber nell'URL con il nome e la porta del server Web su cui si trova CA Service Desk Manager.

Ulteriori informazioni:

[Inclusione dei portlet](#) (a pagina 572)

Integrazione di prodotti Mainframe

I dati lato CA Service Desk Manager (file con estensione dat) sono associati alle integrazioni di prodotti mainframe.

Caricamento dati lato CA Service Desk Manager

I dati lato CA Service Desk Manager (file con estensione dat) associati alle integrazioni di prodotti mainframe sono contenuti in un elenco che associa un file con estensione dat al nome del prodotto mainframe.

Nota: per impostazione predefinita, il server CA Service Desk Manager viene configurato per l'utilizzo della metodologia ITIL. È tuttavia necessario applicare gli aggiornamenti di ITIL ai dati di integrazione. Utilizzare *pdm_userload -a itil_integXXX.dat* per applicare gli aggiornamenti solo dopo il caricamento del rispettivo file integXXX.dat.

Utilizzare *pdm_userload -f integXXX.dat* per caricare i dati lato CA Service Desk Manager per l'abilitazione di una particolare integrazione. I file vengono trasferiti in \$NX_ROOT\data\integrations\.

Nota: per ulteriori informazioni sull'attivazione del lato di chiamata (lato del prodotto mainframe) dell'integrazione, vedere *CA Common Services per z/OS - Guida all'integrazione di CA Service Desk*.

Prodotti CA che utilizzano CAISDI

Nella tabella seguente sono elencati i prodotti mainframe CA che utilizzano CAISDI e i file con estensione dat associati:

Prodotto CA	File dati primari	File aggiornamento ITIL
CA Advantage EDBC	integEDBC.dat	
CA 1 Tape Management	integCA1.dat	itil_integCA1.dat
CA Allocate DASD Space and Placement	integAllocate.dat	itil_integAllocate.dat
CA Disk Backup and Restore	integDisk.dat	itil_integDisk.dat
CA TLMS Tape Management (CA TLMS)	integTLMS.dat	itil_integTLMS.dat
CA Vantage Storage Resource Manager (CA Vantage SRM)	integVantage.dat	itil_integVantage.dat
CA 7 Workload Automation (CA 7 WA)	integCA7.dat	itil_integCA7.dat
CA JARS Resource Accounting (CA JARS RA)	integJARS.dat	itil_integJARS.dat
	integJARSMVS.dat	itil_integJARSMVS.dat
CA MIM Resource Sharing (CA MIM RS)	integMIM.dat	itil_integMIM.dat
CA OPS/MVS Event Management and Automation (CA OPS/MVS EMA)	integOPSMVS.dat	itil_integOPSMVS.dat

CA SYSVIEW Performance Management (CA SYSVIEW)	integSysview.dat	itil_integSysview.dat
CA NetMaster Network Management per TCP/IP (CA NetMaster NM per TCP/IP)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster Network Management per SNA (CA NetMaster NM per SNA)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster Network Automation (CA NetMaster NA)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster Network Operations per TCP/IP (CA NetMaster NO per TCP/IP)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster File Transfer Management (CA NetMaster FTM)	integNetMaster.dat	itil_integNetMaster.dat
CA MICS Resource Management (CA MICS)	integNeuMICS.dat	itil_integNeuMICS.dat

Pianificazione dei prodotti CA per l'uso di CAISDI

Nella tabella seguente sono elencati i prodotti mainframe CA che utilizzano CAISDI e i file con estensione dat associati:

Prodotto CA	File dati primari	File aggiornamento ITIL
CA 2E	integ2e.dat	
CA Enterprise Workload Automation	integAutoSys.dat	
CA Bundl	integBundl.dat	
CA 11 Enterprise Workload Automation Restart and Tracking	integCA11.dat	
CA Connect	integConnect.dat	
CA Datamacs	integDatamacs.dat	
CA Date Simulator	integDate.dat	
CA Deliver	integDeliver.dat	itil_integDeliver.dat
CA Dispatch	integDispatch.dat	itil_integDispatch.dat
CA FAVER VSAM Data Protection	integFaver.dat	
CA FileAge	integFileAge.dat	
CA File Master Plus	integFileMaster.dat	

CA Filesave RCS Automated Recovery	integFileSave.dat	
CA Gen	integGen.dat	
CA GSS (componente comune)	integGSS.dat	
CA InterTest	integInterTest.dat	
CA JCLCheck Enterprise Workload Automation	integJCLCheck.dat	
CA Jobtrac Job Management	integJobtrac.dat	itil_integJobtrac.dat
CA LPD Report Convergence	integLPD.dat	
CA Optimizer	integOptimizer.dat	
CA Optimizer/II	integOptimizerII.dat	
CA Plex	integPlex.dat	
CA Scheduler Job Management	integScheduler.dat	
CA Spool Enterprise Print Management	integSpool.dat	itil_integSpool.dat
CA SymDump	integSymDump.dat	
CA Verify	integVerify.dat	
Visualizzazione CA	integView.dat	itil_integView.dat

Integrazione di CA Service Desk Manager con SAP Solution Manager

L'integrazione di CA Service Desk Manager con SAP Solution Manager fornisce un ambiente di supporto caratterizzato dai seguenti vantaggi:

- Fornisce un'origine definitiva per tutti gli incidenti all'interno dell'organizzazione.
Gli incidenti di CA Service Desk Manager vengono replicati automaticamente in SAP Solution Manager.
- Fornisce agli utenti finali e agli analisti una visione di insieme di tutti gli incidenti in CA Service Desk Manager.
- Consente la sincronizzazione in tempo reale degli incidenti in entrambi i prodotti.
- Sincronizza i record contatto creati in CA Service Desk Manager oppure in SAP Solution Manager.
- Semplifica la conformità ai controlli Sarbanes-Oxley (SOX) offrendo un approccio consolidato alla gestione di incidenti, problemi, richieste, cambiamenti e configurazioni.
- Consente un reporting centralizzato.

Importante Se si richiede l'assistenza di CA per questa integrazione, CA fornirà supporto per il codice CA Service Desk Manager e sarà responsabile solo della parte CA Service Desk Manager dell'integrazione. Si consiglia vivamente di richiedere l'assistenza di un membro di un team SAP Basis per l'implementazione della parte SAP dell'integrazione per verificare che la configurazione sia corretta.

Prerequisiti per l'integrazione

È consigliabile comprendere i limiti imposti da SAP sull'automazione e la riconciliazione dei dati esaminando la documentazione relativa all'implementazione SAP.

Importante I campi relativi al nome, al cognome e all'indirizzo di posta elettronica di tutti i contatti *devono* essere popolati in CA Service Desk Manager e SAP Solution Manager. Se si crea un ticket in CA Service Desk Manager con un utente che presenta uno di questi campi vuoto, il ticket non viene propagato correttamente in SAP Solution Manager. Per ulteriori informazioni sulla gestione dei contatti per le integrazioni, consultare la *SAP Solution Manager 3rd Party Helpdesk Integration Guide*.

Nota: è possibile impostare questi attributi nel modo appropriato con Web Screen Painter. Per ulteriori informazioni sull'utilizzo di questa applicazione, vedere la *Guida di Web Screen Painter*.

Prima di eseguire l'integrazione con SAP Solution Manager, considerare i prerequisiti seguenti:

- Recuperare le informazioni seguenti dall'ambiente CA Service Desk Manager r12.1 o r12.5:

- URL WSDL
- Valore GUID di CA Service Desk Manager

Impostazione predefinita: CA00000000000000000000000000000000

- Utente SAP di sistema predefinito e relative informazioni di accesso

- Pacchetto di installazione CA

Il pacchetto di installazione si trova nella directory degli esempi di CA Service Desk Manager. Il file C000020200009_0000009.SAR si trova ad esempio in `$NX_ROOT\samples`.

Nota: il nome di questo file .SAR può cambiare ma il file deve rimanere nel percorso `$NX_ROOT\samples`.

- Valore della categoria CA Service Desk Manager corrente che è possibile ottenere dall'amministratore o eseguendo il comando seguente sul server CA Service Desk Manager:

```
pdm_extract -f "select persid, sym from Prob_Category"
```

Questo comando visualizza il valore ID persistente e il relativo mapping alla categoria di riferimento. Selezionare una di queste categorie con il relativo ID per popolare la categoria predefinita per gli incidenti SAP generati da SAP in CA Service Desk Manager.

- Completare e testare una configurazione di base di SAP Solution Manager SP14 e SAP Front End Launch Pad Versione 7.10 SP13 (versioni minime richieste).

Nota: nelle versioni precedenti di SAP Front End esiste un problema noto relativo al trasporto utilizzato per le importazioni dei pacchetti.

- Conoscenza operativa di WebAS, SOAMANAGER e ABAP Workbench
- Ottenere l'ID di accesso SAP utilizzato per l'installazione. Tale ID *deve* disporre delle autorizzazioni per l'esecuzione delle transazioni seguenti:
 - /nSAINT
 - /nSOAMANAGER
 - /nSICF
 - /nSE80

- /nSM59
- /nSCPR20
- Gestire la posta elettronica per il Business Partner che intende utilizzare CA Service Desk Manager.
- Confermare la disponibilità dei requisiti e delle condizioni per l'importazione SAP:
 - BBPCRM 500 (obbligatorio)
 - SAP_ABAP 700 (obbligatorio)
 - SAP_BASIS 700 (obbligatorio)
- Verificare di disporre delle revisioni minime richieste per i pacchetti, le patch e i service pack SAP:
 - SAPKIPYJ7E
 - SAPKITL425
 - SAPKITLQ16
 - SAPKNA7011
 - SAPKU50011
 - SAPKA70014
 - SAPKB70014
 - PI_BASIS - 2005_1_700
 - SAP_AP 700
 - ST 400
 - ST-A/PI 01K_CRM560
 - ST-ICO 150_700
 - ST-PI 2005_1_700
 - ST-SER-700_2008_1

Scenari di integrazione

CA Service Desk Manager memorizza l'identificatore *SAPPersonID* come parte del record contatto. SAP Solution Manager utilizza l'identificatore *SAPPersonID* come identificatore univoco per un record contatto. Gli UUID dei contatti creati in CA Service Desk Manager popolano SAP e ogni volta che viene generato un contatto in CA Service Desk Manager, SAP Solution Manager verifica che l'UUID corrisponda al record contatto SAP utilizzato in un incidente tra i due sistemi.

Si consiglia di impostare questi attributi dei contatti come *richiesto*, dopo aver verificato che l'integrazione sia stata completata correttamente. Se si impostano questi campi dei record contatto come *richiesto* prima di verificare l'integrazione, in alcuni ambiente potrebbe verificarsi un malfunzionamento dei processi operativi.

L'integrazione dell'ambiente CA Service Desk Manager con SAP Solution Manager supporta i seguenti scenari:

SAP Solution Manager controlla il ciclo di vita degli incidenti

Indica il funzionamento continuo di un processo di supporto incidenti SAP maturo, senza interruzioni per l'organizzazione. Dopo l'aggiornamento degli incidenti creati da SAP, gli incidenti vengono sincronizzati con CA Service Desk Manager per supportare un unico repository di tutti gli incidenti all'interno dell'organizzazione.

Questo scenario riduce al minimo il rischio di controlli SOX, poiché l'unico repository contiene una sola origine per tutti gli incidenti all'interno dell'intera organizzazione, anziché due o più repository di incidenti separati (ad esempio SAP Solution Manager e CA Service Desk Manager per altri tipi di ticket).

Gli incidenti di CA Service Desk Manager vengono propagati automaticamente a SAP Solution Manager

Propaga gli incidenti di CA Service Desk Manager a SAP ed espone ai clienti un unico punto di immissione per tutti gli incidenti, anziché lasciare che utenti finali o analisti decidano con quale strumento di supporto aprire gli incidenti.

Nota: questo scenario presenta gli stessi vantaggi illustrati nello scenario precedente.

Nota: per gli incidenti aperti, CA Service Desk Manager e SAP Solution Manager sincronizzano ulteriori informazioni che aggiungono automaticamente dati SAP all'incidente di CA Service Desk Manager. Tali informazioni aggiuntive includono modifiche apportate ai valori Priorità, Assegnatario, Commenti e Descrizione e la maggior parte dei dati SAP necessari per fornire assistenza da entrambi i prodotti.

Ulteriori informazioni:

[Modalità di controllo del ciclo di vita di un incidente da parte di SAP Solution Manager: esempio](#) (a pagina 586)

[Modalità di propagazione di incidenti a SAP Solution Manager: esempio](#) (a pagina 586)

Modalità di controllo del ciclo di vita di un incidente da parte di SAP Solution Manager: esempio

Il seguente esempio di scenario di integrazione dimostra come SAP Solution Manager controlla il ciclo di vita degli incidenti:

1. Un cliente segnala un incidente SAP nell'ambiente SAP.
2. SAP crea un messaggio di supporto per l'incidente.
3. SAP replica automaticamente l'incidente in CA Service Desk Manager, con una categoria specifica che indica che l'incidente è stato generato ed è gestito da SAP.
4. Un membro del team SAP valuta il report dell'incidente.
5. Il team SAP gestisce e aggiorna l'incidente con una soluzione proposta.
6. La soluzione proposta viene inoltrata a CA Service Desk Manager solo a titolo informativo.
7. Il team SAP rivede la soluzione proposta con l'autore del report sull'incidente.
8. Se la soluzione proposta non risolve l'incidente, si verifica quanto segue:
 - a. SAP rifiuta la soluzione.
 - b. SAP inoltra automaticamente il rifiuto a CA Service Desk Manager solo a titolo informativo.
 - c. SAP gestisce l'incidente finché non viene identificata un'altra soluzione proposta e l'elaborazione continua ritornando al passaggio 5.
9. Se la soluzione proposta risolve l'incidente, si verifica quanto segue:
 - a. SAP aggiorna l'incidente per dimostrare che la soluzione funziona.
 - b. SAP inoltra automaticamente l'aggiornamento dell'incidente a CA Service Desk Manager solo a titolo informativo.
 - c. SAP chiude l'incidente.
 - d. SAP inoltra a e chiude automaticamente l'incidente in CA Service Desk Manager.

Modalità di propagazione di incidenti a SAP Solution Manager: esempio

Il seguente esempio di scenario di integrazione dimostra come gli incidenti di CA Service Desk Manager vengono propagati automaticamente a SAP Solution Manager:

1. Un cliente segnala un incidente.
2. CA Service Desk Manager crea un messaggio di supporto per l'incidente.

3. Un membro del team CA Service Desk Manager valuta il report dell'incidente.
4. Se il membro del team CA Service Desk Manager stabilisce che l'incidente è specifico di SAP, CA Service Desk Manager lo contrassegna come rilevante per SAP e lo inoltra a SAP.
5. SAP crea l'incidente.
6. Il team SAP valuta l'incidente.
7. Il team SAP gestisce l'incidente e dopo che viene identificata una possibile soluzione, SAP invia i dettagli della soluzione proposta a CA Service Desk Manager.
8. Il team CA Service Desk Manager rivede la soluzione proposta con l'autore del report sull'incidente.
9. Se la soluzione proposta non risolve l'incidente, si verifica quanto segue:
 - a. CA Service Desk Manager rifiuta la soluzione.
 - b. CA Service Desk Manager inoltra il rifiuto a SAP.
 - c. SAP gestisce l'incidente finché non viene identificata un'altra soluzione proposta e l'elaborazione continua ritornando al passaggio 7.
10. Se la soluzione proposta risolve l'incidente, si verifica quanto segue:
 - a. CA Service Desk Manager aggiorna l'incidente per dimostrare che la soluzione funziona.
 - b. CA Service Desk Manager chiude l'incidente.
 - c. CA Service Desk Manager inoltra la chiusura dell'incidente a SAP.
 - d. SAP chiude automaticamente l'incidente.

Modalità di integrazione con SAP Solution Manager

Importante Le schermate visualizzate in questa integrazione si basano sulle versioni di SAP Solution Manager e CA Service Desk Manager disponibili al momento della pubblicazione. Tali schermate potrebbero essere diverse da quelle dell'ambiente SAP in uso.

Per integrare CA Service Desk Manager con SAP Solution Manager procedere nel modo seguente:

1. [Installare](#) (a pagina 588) il connettore CA Service Desk (CASD).

Per decomprimere e installare il file di installazione, utilizzare lo strumento SAP Add-On Installation Tool (transaction SAINT).
2. [Attivare](#) (a pagina 592) i Business Configuration Set (BC Set).

L'attivazione dei BC Set consente di semplificare il processo di immissione nel workbench e di personalizzazione delle voci di tabella.

3. [Configurare](#) (a pagina 593) SAP Solution Manager.

Creare un utente con privilegi in SAP, configurare la connessione al servizio Web in entrata e impostare la categoria CA Service Desk Manager predefinita per gli incidenti avviati in SAP Solution Manager.

4. [Configurare](#) (a pagina 602) CA Service Desk Manager.

Completare la connessione al servizio Web, installare le opzioni SAP in CA Service Desk Manager e configurare l'utente con privilegi nel sistema operativo e in CA Service Desk Manager.

5. Verificare che l'integrazione sia stata configurata correttamente.

Per assicurarsi che la connessione e l'integrazione siano state eseguite correttamente, [tenere traccia dei ticket](#) (a pagina 609) creati in CA Service Desk Manager o in [SAP Solution Manager](#) (a pagina 607) .

Modalità di installazione di CASD Connector

CASD Connector (CA Service Desk Connector) contiene una raccolta di oggetti ABAP e componenti di configurazione funzionale personalizzati. CASD Connector elabora i messaggi di supporto generati e aggiornati sia da CA Service Desk Manager che da SAP Solution Manager. SAP Add-on Assembly Tool Kit (AAK) assembla il contenuto di CASD Connector per la consegna e crea il file di pacchetto (.PAT).

Per installare il pacchetto SAP, procedere come segue:

1. Accedere al Client 000 in SAP Solution Manager.
2. [Eseguire SAP Add-On Installation Tool](#) (a pagina 589) (transazione SAINT).
3. Individuare e [decomprimere](#) (a pagina 589) il file di installazione (.SAR) sul computer front-end.
4. [Installare](#) (a pagina 590) il file di installazione decompresso (.PAT) sul server applicazioni.
5. Disconnettersi dal Client 000.

È possibile accedere al Client 100 per attivare i Business Connector Set in SAP Solution Manager.

Esecuzione di SAP Add-On Installation Tool (transazione SAINT)

Importante Le schermate acquisite visualizzate in questa integrazione sono basate sulle release di SAP Solution Manager e CA Service Desk Manager disponibili al momento della pubblicazione. Le schermate riportate di seguito potrebbero differire da quelle dell'ambiente SAP in uso.

Accedere a SAP Solution Manager ed eseguire SAP Add-On Installation Tool (transazione SAINT) per preparare l'installazione del pacchetto per integrazione di CA Service Desk Manager e SAP.

Per eseguire la transazione SAINT

1. Accedere al Client 000.
2. Nel menu File, selezionare System, Status per verificare di essere connessi al Client.

Viene visualizzato lo stato del sistema e dati di sola lettura relativi al Client 000, ad esempio dati di utilizzo, dati SAP, dati dell'host e così via.
3. Chiudere la finestra dello stato di sistema dopo aver verificato di essere connessi al Client 000.
4. Immettere il codice transazione **/nsaint** e fare clic su Execute.

In questa integrazione è necessario immettere ogni transazione nel campo di comando e fare clic sull'icona Execute, come indicato di seguito:

Viene eseguita la transazione SAINT ed è possibile iniziare a decomprimere il pacchetto di installazione dal menu File.

Decompressione del file di installazione

Dopo l'esecuzione della transazione SAINT, viene visualizzato un menu File che consente di individuare e decomprimere il file di installazione e di caricarlo sul server applicazioni di destinazione. Il pacchetto di installazione si trova nella directory degli esempi di CA Service Desk Manager. Ad esempio, il file *C000020200009_0000009,SAR* si trova nella directory `$NX_ROOT\samples`. È possibile copiare sul server il file di installazione compresso.

Nota: il nome di file *C000020200009_0000009,SAR* può variare, ma è possibile individuarlo nella directory `$NX_ROOT\samples`.

Per individuare e decomprimere il file

1. Nel menu File, fare clic su Installation Package, Load packages, From Front End.

Viene visualizzata la finestra di dialogo Select CAR/SAR archive che consente di accedere alla directory degli esempi sul server CA Service Desk Manager.

2. Individuare il file di installazione compresso sul computer front-end e fare clic su Open.

Nella parte inferiore dello schermo viene visualizzato un messaggio che informa che è in corso il caricamento del file .SAR dalla workstation.

Viene visualizzato il contenuto della finestra del file compresso c000020200009_0000009.sar e viene elencato il file di installazione C000020200009_0000009.PAT decompresso.

3. Fare clic su Decompress.

Il file viene decompresso e il file .PAT viene caricato nella directory appropriata sul server applicazioni di destinazione.

Viene visualizzato un messaggio che conferma l'installazione dei componenti aggiuntivi e del sistema preconfigurato e informa che è possibile installare CASD Connector.

Installazione di CASD Connector

Al termine della decompressione del file di installazione, è possibile installare CASD Connector.

Per installare CASD Connector

1. Fare clic su Start al termine della decompressione del file di installazione.
Viene visualizzata una pagina che contiene i pacchetti aggiuntivi installabili. In questo esempio, il componente aggiuntivo è *CASD 100_710: Add-On Installation*.

2. Selezionare la riga del pacchetto *CASD 100_710: Add-On Installation* e fare clic su Continue.

Il pacchetto di installazione calcolato viene visualizzato nella scheda Support Package. Ad esempio, il pacchetto calcolato è *SAPK-100COINCASD*.

Nota: non è necessario un altro pacchetto di supporto per questa installazione.

3. Fare clic su Continua.

Viene visualizzata la scheda della coda di installazione che mostra il pacchetto OCS *SAPK-100COINCASD*.

4. Fare clic su Continua.

Viene visualizzata una finestra di dialogo che chiede se si desidera aggiungere "Modification Adjustment Transports" alla coda.

Importante Se viene visualizzata questa finestra di dialogo, fare clic su No.

Viene visualizzata la schermata di richiesta della password SAINT che chiede di specificare la password per il pacchetto OCS SAPK-100COINCASD.

5. Immettere **8DF4AF33AE** e fare clic su Execute.

Viene visualizzata la schermata SAINT: Add-on installation che conferma che è in corso l'installazione del *pacchetto Add-On CASD rel. 100_710*.

6. Per continuare, fare clic sull'icona che raffigura un segno di spunta verde.

Viene visualizzare la schermata Add-on CASD Rel. 100_710 che indica che il componente aggiuntivo è stato importato.

7. Fare clic su Fine.

Un messaggio visualizzato nella parte inferiore dello schermo indica che l'installazione del componente aggiuntivo è stata completata.

8. Disconnettersi dal Client 000.

L'installazione di CASD Connector è terminata ed è ora possibile attivare i Business Connector Set in SAP Solution Manager sul Client 100.

Nota: per la restante parte di questa integrazione, accedere al Client 100.

Business Configuration Set

CASD Connector fornisce tre Business Configuration Set (BC Set) per il sistema SAP Solution Manager. I BC Set semplificano il processo di immissione di voci di tabella del workbench e di personalizzazione. Queste voci sono necessarie per configurare il sistema per l'utilizzo di CASD Connector.

Vengono forniti al sistema i seguenti BC Set:

- /CASD/HIERARCHY

Specifica un BC Set gerarchico contenente i seguenti BC Set.

- /CASD/WORKBENCH

Specifica un BC Set semplice creato da richieste del workbench.

- /CASD/CUSTOMIZING

Specifica un BC Set semplice creato da richieste di personalizzazione.

Attivazione dei Business Configuration Set

Se si ha accesso al client di installazione e si dispone delle autorizzazioni necessarie per eseguire la transazione SCPR20, attivare i BC Set forniti con l'installazione di CASD Connector. Attivando il BC Set gerarchico, vengono attivati anche i BC Set del workbench e di personalizzazione.

Per attivare i BC Set

1. Accedere al Client 100.

2. Eseguire la transazione */nscpr20*.

Viene visualizzata la pagina Business Configuration Sets: Activate.

3. Immettere */CASD/Hierarchy* come nome del BC Set e premere Invio.

Nota: è possibile immettere ***CASD*** come nome del BC Set per facilitare la ricerca di BC Set.

4. Nel menu File, fare clic su BC Set, Activate.

Viene visualizzata la finestra Prompt for Workbench request.

5. Fare clic sull'icona Create per creare la richiesta del workbench, come indicato nell'esempio seguente:

Importante Non utilizzare una richiesta esistente, anche se il sistema ne propone una.

Viene visualizzata la finestra Create Request.

6. Immettere *BC Set Activation Workbench Request* come descrizione breve e fare clic su Save.

Viene nuovamente visualizzata la finestra Prompt for Workbench request.

7. Prendere nota del numero di trasporto *Q00K900006* visualizzato nella pagina Prompt for Workbench request e fare clic sul segno di spunta verde per continuare.

Viene visualizzata la finestra Prompt for Customizing request.

8. Fare clic sull'icona Create (come indicato nell'immagine precedente).

Importante Non utilizzare una richiesta esistente, anche se il sistema ne propone una.

Viene visualizzata la finestra Create Request.

9. Immettere *BC Set Activation Customizing Request* come descrizione breve e fare clic su Save.

Viene nuovamente visualizzata la finestra Prompt for Customizing request.

10. Prendere nota del numero di trasporto *Q00K900008* visualizzato nella pagina Prompt for Customizing request e fare clic sul segno di spunta verde per continuare.

Viene visualizzata la finestra Activation Options. Selezionare l'opzione appropriata, come indicato nel seguente esempio:

- Fare clic sull'icona che raffigura un segno di spunta verde per eseguire l'attivazione e generare un file di registro.
- Fare clic sull'icona rossa Cancel With Log per eseguire un'attivazione di prova e generare un file di registro.

Viene visualizzato un messaggio che indica che l'attivazione è stata eseguita ed è ora possibile fare clic sull'icona Activation Logs per visualizzare i risultati del BC Set gerarchico.

11. Disconnettersi dal Client 100.

Modalità di configurazione di SAP Solution Manager

Importante Le schermate visualizzate in questa integrazione si basano sulle versioni di SAP Solution Manager e CA Service Desk Manager disponibili al momento della pubblicazione. Tali schermate potrebbero essere diverse da quelle dell'ambiente SAP in uso.

Nei passaggi seguenti viene riepilogata la modalità di configurazione di SAP Solution Manager dopo aver installato il connettore CASD e attivati i BC Set:

1. Verificare che i [servizi](#) (a pagina 594) APPL_SOAP_MANAGEMENT e WSDL siano attivi.
2. Creare l'[ID utente RFC](#) (a pagina 595) che esegue i servizi SAP Solution Manager per CA Service Desk Manager.
3. Configurare il servizio Web [/CASD/CA_SD_WS in entrata](#) (a pagina 595) che gestisce il servizio Web in entrata per CA Service Desk Manager.
[Attivare il servizio Web /CASD/CA_SD_WS](#) (a pagina 596) per la connessione a CA Service Desk Manager e SAP Solution Manager.
4. Testare il servizio Web utilizzando Web Services (WS) Navigator per verificarne il corretto funzionamento.
5. Configurare il proxy del [client in uscita](#) (a pagina 598) per creare la porta logica e generare una destinazione RFC.

Configurare la [destinazione RFC](#) (a pagina 600) in modo che SAP Solution Manager possa indirizzare correttamente la chiamata in uscita a CA Service Desk Manager.

6. Configurare la [connessione da SAP Solution Manager](#) (a pagina 600) a CA Service Desk Manager in modo da poter configurare CA Service Desk Manager per l'integrazione.

Modificare la [categoria CA Service Desk Manager predefinita](#) (a pagina 601) per gli incidenti avviati da SAP in modo da poter sincronizzare correttamente gli incidenti in SAP Solution Manager e CA Service Desk Manager.

Attivazione dei servizi SOAMANAGER

L'attivazione dei servizi SOAMANAGER viene eseguita dopo la configurazione dei Business Configuration Set. Questi servizi attivano il sito HTTP per SAP Solution Manager e generano il documento WSDL.

Per attivare i servizi SOAMANAGER

1. Eseguire la transazione `/nSICF`.
Viene visualizzato l'elenco dei servizi.
2. Selezionare il servizio, fare clic con il pulsante destro del mouse su di esso e scegliere Activate Service (Attiva servizio), come illustrato nell'esempio che segue:

Al prompt, fare clic su Yes (Sì).

Il servizio viene attivato.

3. Verificare che i servizi seguenti siano stati attivati.

APPL_SOAP_MANAGEMENT

Attiva il sito HTTP per SAP Solution Manager.

`/sap/bc/webdynpro/sap/APPL_SOAP_MANAGEMENT`

WSDL

Attiva la generazione WSDL del processore SOAP 7.10 che genera la transazione WSDL SOAMANAGER.

`/sap/bc/srt/wSDL`

I servizi sono attivati.

Creazione dell'ID utente RFC

È possibile creare l'ID utente RFC dopo l'attivazione dei servizi SOAMANAGER. Questo utente esegue i servizi di SAP Solution Manager per CA Service Desk Manager.

Per creare l'ID utente RFC

1. Eseguire la transazione */nSU01*.
Viene visualizzata la pagina Display User che consente di configurare l'ID utente RFC.
2. Immettere **CASD_RFC_USR** come utente.
3. Nella scheda Logon data, selezionare il tipo di utente *Communications Data*.
CA Service Desk Manager utilizza l'utente che esegue una chiamata a SAP Solution Manager Service Desk.
4. Verificare che l'utente disponga delle autorizzazioni appropriate per SAP Solution Manager Service Desk.
5. Nella scheda Profiles, assegnare il profilo *SAP_ALL* e salvare l'utente.
L'ID utente RFC è stato creato ed è ora possibile configurare il servizio Web in entrata.

Configurazione del servizio Web in entrata

Utilizzare SOA Management per gestire il servizio Web in entrata per CA Service Desk Manager. Definire l'endpoint del servizio in entrata in modo da connettere CA Service Desk Manager e SAP Solution Manager.

Per configurare il servizio Web in entrata

1. Eseguire la transazione */nSOAMANAGER*.
Dopo l'avvio del browser Web, viene visualizzato il prompt di accesso a SOA Management.
2. Effettuare l'accesso come utente *j2ee_admin*.
3. Nella scheda Business Administration (Amministrazione aziendale) selezionare Web Service Administration (Amministrazione servizio Web), come illustrato nell'esempio seguente:

Viene visualizzata la pagina Web Service Administration (Amministrazione servizio Web).

4. Cercare la definizione di `/CASD/CA_SD_WS` e selezionarla nell'elenco.
Fare clic su **Apply Selection** (Applica selezione).
Fare clic su **Create Service** (Crea servizio) come illustrato nell'esempio seguente:

Viene visualizzata la schermata di SOA Management che consente di immettere informazioni sul servizio e sul binding.

5. Completare le seguenti informazioni:
 - **New Service Name** (Nuovo nome servizio): immettere **ZCA_SD_WS**.
 - **Description** (Descrizione): immettere **CA Inbound WS Adapter**.
 - **New Binding Name** (Nuovo nome di binding): immettere **ZCA_SD_WS**.Fare clic su **Apply Settings** (Applica impostazioni).
6. Nella scheda **Provider Security** (Protezione provider) selezionare *User ID/Password* (ID utente/Password) come metodo di autenticazione e fare clic su **Save** (Salva), come illustrato nell'esempio seguente:

La definizione del servizio viene salvata ed è possibile attivarla.

Attivazione del servizio Web in entrata

Dopo aver attivato `ZCA_SD_WS`, procedere alla configurazione del servizio Web per verificare che la connessione sia stata eseguita correttamente.

1. Eseguire la transazione `/nSICF` ed effettuare le operazioni seguenti:
 - a. Verificare che tutti i servizi padre siano attivi per la struttura seguente:
`/sap/bc/srt/rfc/CASD/CA_SD_WS/`
 - b. Selezionare un servizio, fare clic con il pulsante destro del mouse sul servizio e scegliere **Activate Service** (Attiva servizio).
Nell'esempio seguente viene mostrata la struttura del servizio Web:

Fare clic su **Yes (Sì)** dal prompt.

Il servizio viene attivato ed è pronto per il test.

2. Eseguire la transazione `/nSOAMANAGER`.
Dopo l'avvio del browser Web, viene visualizzata la pagina SOA Management.

3. Nella scheda Technical Configuration (Configurazione tecnica) fare clic su System Global Settings (Impostazioni globali sistema).
Viene visualizzata la pagina System Global Settings (Impostazioni globali sistema).
4. Per confermare il nome host e il numero di porta SAP, rivolgersi all'amministratore SAP.
5. Nella scheda Access Information J2EE server (Informazioni accesso server J2EE) fare clic su Edit/Display (Modifica/Visualizza) per immettere il nome host e il numero di porta SAP (se questi campi non sono stati ancora popolati), come illustrato nell'esempio, e fare clic su Save (Salva).

Il server J2EE viene salvato.

6. Verificare che il servizio Web seguente sia in esecuzione.

`/sap/bc/srt/rfc/CASD/SD_ADAPTER_WS`

7. Nella scheda Business Administration (Amministrazione aziendale) di SOA Management fare clic su Web Service Administration (Amministrazione servizio Web).

Viene visualizzata la pagina Web Service Administration (Amministrazione servizio Web).

8. Selezionare il servizio `/CASD/CA_SD_WS` e fare clic su *Open WSDL document for selected binding* (Apri documento WSDL per binding selezionato) nella scheda Overview (Informazioni generali) della pagina Details of Service Definition (Dettagli definizione servizio), come illustrato nell'esempio seguente:

Nel browser Web viene visualizzato il documento WSDL.

9. Copiare l'URL dalla barra degli indirizzi nell'editor di testo corrente. Il collegamento, ad esempio, può essere visualizzato come segue:

`http://sapdev:8000/sap/bc/srt/wsdl/bndg_DE2DD378D6C687F1B94D005056B04977/wsdl11/allinone/ws_policy/document?sap-client=100`

10. Nella scheda Overview (Informazioni generali) della pagina Details of Service Definition (Dettagli definizione servizio) fare clic su *Open Web Service navigator for selected binding* (Apri Web Services Navigator per binding selezionato).

Viene visualizzato il prompt di autenticazione di SOAMANAGER per l'accesso a Web Services Navigator.

11. Effettuare l'accesso come utente `j2ee_admin`.

Viene visualizzato Web Services Navigator.

12. (Facoltativo) Eseguire i passaggi seguenti in Web Services Navigator:

- a. Immettere l'URL WSDL del servizio Web copiato e fare clic su Next (Avanti).
- b. Effettuare l'accesso specificando l'utente *CASD_RFC_USR* [creato in precedenza](#) (a pagina 595).

Viene visualizzata la pagina Web Services Navigator Overview (Informazioni generali Web Services Navigator).

- c. Fare clic su Test.
- d. Eseguire l'operazione sapTest, come illustrato nell'esempio seguente:

Test della connessione ai servizi Web.

- e. Immettere un valore qualsiasi nel prompt RequestMessage, ad esempio *000*.

In risposta alla richiesta 000 viene visualizzato un messaggio quale "Hello World", come illustrato nell'esempio seguente:

Questa risposta conferma che i servizi in entrata sono connessi correttamente.

WSDL può essere utilizzato con CA Service Desk Manager.

Configurazione del proxy per il client in uscita

Una porta logica punta alla destinazione RFC. È possibile creare una porta logica e generare una destinazione RFC in modo che SAP Solution Manager sappia dove dirigere la chiamata in uscita a CA Service Desk Manager.

Per configurare il proxy del client in uscita

1. Eseguire la transazione */nSOAMANAGER*.

Viene avviato il browser Web dell'utente e viene visualizzata la pagina SOA Management.

2. Nella scheda Business Administration, selezionare Web Services Administration.

Viene visualizzata la pagina Web Service Administration.

3. Individuare il proxy del client in uscita */CASD/CO_USD_WEB_SERVICE_SOAP*.

Selezionare */CASD/CO_USD_WEB_SERVICE_SOAP* dall'elenco e fare clic su Apply Selection.

Viene visualizzata la pagina Details of Proxy Definition.

4. Nella scheda Configurations, fare clic su Create Logical Port, come illustrato di seguito:

Viene visualizzata la pagina General Configuration Settings.

5. Selezionare il tipo Manual Configuration.

Attivare l'opzione *Logical Port is Default*.

6. Completare le seguenti informazioni:

- New Service Name—Immettere **zsn_casd**.
- New Binding Name—Immettere **zbn_casd**.
- Logical Port Name—Immettere **CASD_SERVICE_DESK**.

Importante Il nome immesso nel campo Logical Port Name deve essere in lettere maiuscole, ad esempio CASD_SERVICE_DESK.

Fare clic su Apply Settings.

7. Nella scheda Transport settings della pagina Configuration of Web Service, compilare i seguenti campi:

URL Access Path

Immettere **axis/services/USD_R11_WebService** come posizione dell'endpoint CASD.

Importante Non aggiungere una barra ("/") all'inizio del percorso specificato nel campo URL Access Path poiché provoca un errore durante il salvataggio.

Computer Name of Access URL

Immettere il nome host del server CA Service Desk Manager.

Port Number of Access URL

Immettere **8080** come porta CA Service Desk Manager (solo se si dispone di un'installazione CA Service Desk Manager valida).

Nota: la porta CA Service Desk Manager predefinita è 8080, ma si consiglia di rivolgersi all'amministratore di CA Service Desk Manager per conferma.

L'esempio riportato di seguito mostra la scheda Transport Settings:

8. Fare clic su Salva.

La porta logica è stata creata.

Importante In caso di errore durante il salvataggio, uscire completamente da SAP Solution Manager e ripetere la procedura dal passaggio 6.

Configurazione della destinazione RFC

Dopo aver creato la porta logica, SOAMANAGER genera automaticamente una destinazione RFC. È necessario testare la connettività della destinazione RFC prima di configurare la connessione SAP Solution Manager.

Per configurare la destinazione RFC

1. Eseguire la transazione */nSM59*.

Viene visualizzata la pagina Configuration of RFC Connections.

2. Selezionare la connessione RFC dall'elenco.

Ad esempio, la destinazione RFC generata da SOAMANAGER è una stringa esadecimale di 32 caratteri *DE4BE05CF5DA4BF1BDB6005056B04977*.

3. Fare clic su Connection Test.

Viene visualizzata la pagina Connection Test che mostra uno stato HTTP pari a 200, come indicato di seguito:

La connessione RFC è stata configurata.

Configurazione della connessione SAP Solution Manager

Dopo avere configurato la destinazione RFC e testato la connessione, è possibile generare e gestire il GUID CA Service Desk Manager per configurare CA Service Desk Manager con il GUID di sistema di SAP Solution Manager.

Per configurare la connessione SAP Solution Manager

1. Eseguire la transazione */n/casd/guid*.

Viene visualizzata la pagina Maintain CA Service Desk Manager GUID.

2. Immettere il GUID di 32 caratteri e fare clic sull'icona Execute per continuare.

Nota: il valore predefinito del GUID per CA Service Desk Manager è *CA00000000000000000000000000000000*.

Viene visualizzato un messaggio che informa che l'ID GUID è stato aggiornato.

3. Eseguire la transazione */nICTCONF*.

Viene visualizzata la pagina Configure SAP Solution Manager Service Desk Interface.

4. Fare clic sull'icona Generate e selezionare Do Not Overwrite Old Values, come indicato di seguito:
5. Fare clic su Salva.
Viene generato il mapping predefinito ed è possibile fornire a CA Service Desk Manager il GUID di sistema di SAP Solution Manager.
6. Eseguire la transazione `/n/CASD/SOLMAN_GUID`.
Viene visualizzata la pagina Get Solution Manager GUID che visualizza il GUID, ad esempio DE2E02F6B5CAF1F1B94D005056B04977.
Importante Il GUID è un parametro univoco obbligatorio per la configurazione di CA Service Desk Manager.
7. Eseguire la transazione `/n/CASD/AUTH`.
Viene visualizzata la pagina Maintain the username and password for the CASD connector.
8. Immettere il nome utente e la password di CA Service Desk Manager e fare clic su Execute.
Il nome utente e la password per CA Service Desk Manager sono ora gestiti.

Modifica della categoria CA Service Desk Manager predefinita per gli incidenti generati da SAP

Dopo aver configurato la connessione SAP Solution Manager, è necessario immettere i valori predefiniti iniziali in modo che CA Service Desk Manager e SAP Solution Manager possano comunicare. È inoltre possibile modificare la categoria CA Service Desk Manager predefinita per gli incidenti creati in SAP Solution Manager.

Viene definita una categoria CA Service Desk Manager predefinita per il sistema SAP in modo tale che, quando SAP invia e sincronizza incidenti con CA Service Desk Manager, viene impostata automaticamente la categoria dell'incidente. Questa azione non sostituisce la categoria SAP impostata per l'incidente SAP e indicata nella scheda SAP dell'incidente CA Service Desk Manager.

Per modificare le categoria predefinita

1. Eseguire la transazione `/n/CASD/TABLEINIT`.

Viene visualizzata la pagina Initialize some /CASD/SERVICEDESK application data tables, come indicato di seguito:

2. Ottenere il valore corrente della categoria CA Service Desk Manager da utilizzare in SAP Solution Manager.

Nota: per ottenere il valore della categoria, rivolgersi all'amministratore di CA Service Desk Manager oppure eseguire il comando pdm_extract, come illustrato nei prerequisiti di questa integrazione.

3. Eseguire la transazione /nse11 sul server di SAP Solution Manager.

Viene visualizzata la schermata ABAP Dictionary.

4. Selezionare Database table e immettere **/CASD/ATTRIBUTE**, quindi fare clic su Display.

Viene visualizzata la schermata Dictionary: Display Table.

5. Fare clic su Table List, come indicato di seguito:

Viene visualizzata la schermata Data Browser: Table /CASD/ATTRIBUTE: Selection Screen.

6. Fare clic sull'icona Execute .

Viene visualizzata la schermata Data Browser: Table /CASD/ATTRIBUTE Select Entries.

7. Selezionare la riga Category Attribute e fare clic su Table Entry, Change.

Viene visualizzata la schermata Data Browser: Table /CASD/ATTRIBUTE: Selection.

8. Modificare CA_VALUE impostandolo sul persid della categoria di CA Service Desk Manager per generare l'istanza SAP (ad esempio, **pcat:5110**) e fare clic su Save.

Il valore predefinito della Categoria CA Service Desk Manager viene salvato e la tabella /CASD/ATTRBUTE visualizza pcat:5110 come CA_Value.

Modalità di configurazione di CA Service Desk Manager

Per configurare la connessione servizi Web a SAP Solution Manager, attenersi alla seguente procedura in CA Service Desk Manager:

1. Accedere a CA Service Desk Manager.
2. Nella scheda Amministrazione, accedere a Gestione opzioni, SAP.

Viene visualizzato l'Elenco opzioni.

3. Installare e modificare i valori delle seguenti opzioni, come richiesto dall'ambiente in uso:

CASD_GUID

(Obbligatorio) Valore esadecimale di 32 cifre (0-F) che identifica in modo univoco l'istanza SAP CA Service Desk Manager in SAP Solution Manager. Il valore può essere modificato in qualunque momento. Tuttavia, in questo caso è necessario riavviare il server CA Service Desk Manager e riconfigurare SAP Solution Manager, a meno che non si utilizzi il valore predefinito.

Impostazione predefinita: CA00000000000000000000000000000000

SAP_CERT

Consente di specificare il file del certificato predefinito che si connette all'installazione SAP Solution Manager configurata per l'autenticazione basata su certificato per i servizi Web. Il valore può essere modificato in qualsiasi momento, ma occorrerà riavviare il server CA Service Desk Manager.

Nota: l'installazione di questa opzione è *obbligatoria*, sebbene non sia necessario fornire un valore.

SAP_GUID

Specifica il GUID dell'istanza SAP Solution Manager. Il GUID è una stringa di 32 caratteri (0-9, A-F) che identifica in modo univoco la specifica istanza SAP Solution Manager.

SAP_LANG

Riservato per le future versioni localizzate di CA Service Desk Manager.

Nota: fare clic su Modifica e impostare questa opzione su Installa.

SAP_PWD

Specifica la password richiesta da SAP_USER per l'accesso al sistema WSDL/Solution Manager.

SAP_URI

Specifica l'URL iniziale per un'istanza SAP Web Services se è necessario un URL anziché un collegamento a SAP_WSDL. L'URL viene fornito all'amministratore Service Desk dal team SAP Basis (Supporto) dopo la corretta installazione e configurazione del pacchetto SAP .SAR. L'URL può essere modificato in qualsiasi momento, ma occorrerà riavviare il server CA Service Desk Manager.

SAP_USER

Specifica il nome utente che dispone dell'accesso appropriato a Web Services per l'integrazione.

Esempio: CASD_RFC_USR

SAP_WSDL

Specifica il percorso al file WSDL, ad esempio

file:///c:/Program%20Files/CA/SAP.wsd/ o il seguente URL di esempio:

http://sapdev.ca.com:8000/sap/bc/srt/wsdll/bndg_DE2DD378D6C687F1B94D005056B04977/wsdll1/allinone/ws_policy/document?sap-client=100

4. Nella scheda Amministrazione, fare clic su Norma dei servizi Web, Norme.
Viene visualizzato l'Elenco norme di accesso servizi Web.
5. Modificare la norma *IMPOSTAZIONE PREDEFINITA* come indicato di seguito:
 - a. Stato—Selezionare Attivo.
 - b. Contatto proxy—"ServiceDesk, CA"
 - c. Selezionare la casella di controllo Predefinito.
 - d. Selezionare la casella di controllo Consenti rappresentazione.
 - e. Nella scheda Controllo accesso, impostare tutti i campi Operazioni per ora su -1.
 - f. Salvare la norma.La norma viene salvata.
6. Riavviare i servizi CA Service Desk Manager.
La configurazione di CA Service Desk Manager per l'integrazione è stata completata.

Modalità di test dell'integrazione

Nei passaggi seguenti viene riepilogata la procedura di impostazione di un test dell'integrazione:

1. Creare un utente (*sapadm*) (a pagina 605) con i privilegi appropriati sul server CA Service Desk Manager.
2. [Creare un contatto](#) (a pagina 605) in CA Service Desk Manager con i privilegi appropriati.
3. Creare un'[area richiesta/incidente/problema](#) (a pagina 606) che propaghi i ticket in SAP Solution Manager.

Creazione di un utente con privilegi sul server primario (Windows)

Al termine della configurazione di CA Service Desk Manager per l'integrazione, è possibile creare un utente (*sapadm*) nel sistema operativo che dispone di accesso con privilegi sul server CA Service Desk Manager primario. L'utente *sapadm* viene utilizzato per creare un contatto con privilegi in CA Service Desk Manager.

Per creare un utente con privilegi in Windows

1. Accedendo come amministratore, fare clic con il pulsante destro del mouse su Risorse del computer e scegliere Gestisci.
Viene visualizzato lo strumento Gestione computer.
2. Accedere a Utilità di sistema, Utenti e gruppi locali.
Fare clic con il pulsante destro del mouse su Utenti e scegliere Nuovo utente.
Viene visualizzata la finestra di dialogo Nuovo utente.
3. Procedere come segue:
 - Impostare il nome utente su *sapadm*.
 - Impostare una password valida.
4. Deselezionare l'opzione *Cambiamento obbligatorio password all'accesso successivo*.
5. Selezionare le seguenti opzioni:
 - Cambiamento password non consentito
 - Nessuna scadenza password
6. Fare clic su Crea.
L'utente *sapadm* è stato creato.

Creazione di un contatto per l'utente SAP

Dopo aver definito l'utente *sapadm*, è possibile creare un contatto CA Service Desk Manager con i privilegi appropriati.

Per creare un contatto

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Contatti.
Viene visualizzata la pagina Ricerca contatto.
2. Fare clic su Crea nuovo.
Viene visualizzata la pagina Crea nuovo contatto.

3. Inserire i dati nei seguenti campi:
 - Cognome: System_SAP_User
 - Stato: Attivo
 - ID contatto: sapadm
 - Accesso di sistema: sapadm
 - Tipo contatto: Analista
 - Tipo di accesso: Amministrazione
4. Salvare il contatto.
Il contatto viene salvato.

Creazione di un'area ticket che viene propagata a SAP Solution Manager

È possibile creare un'area richiesta/incidente/problema in CA Service Desk Manager in modo che i ticket ad essa assegnati vengano propagati a SAP Solution Manager. Le aree ticket con questa opzione attivata vengono risolte in SAP Solution Manager.

Il sistema SAP crea un messaggio in Solution Manager e aggiorna automaticamente il ticket di CA Service Desk Manager con le informazioni appropriate, ad esempio il numero di messaggio, l'assegnatario e così via.

Per creare un'area ticket per SAP

1. Nella scheda Amministrazione, selezionare Service Desk, Richieste/Incidenti/Problemi, Aree.
Viene visualizzato l'Elenco aree richiesta/incidente/problema.
2. Fare clic su Crea nuovo.
Viene visualizzata la pagina Crea nuova area richiesta/incidente/problema.
3. Compilare i campi appropriati per l'area.
Ad esempio, immettere **Accesso SAP** come simbolo e selezionare l'area ticket in modo che sia valida solo per gli incidenti e non per le richieste o i problemi.
4. Selezionare l'opzione Propaga a SAP.
5. Salvare l'area ticket e chiudere la finestra.
L'area ticket viene salvata.

Creazione di un ticket CA Service Desk Manager in SAP Solution Manager

Se si desidera che SAP Solution Manager controlli il ciclo di vita dei ticket, creare i ticket CA Service Desk Manager utilizzando il menu Help (?) di SAP Solution Manager. I ticket, ad esempio gli incidenti, avviati in SAP vengono sincronizzati con CA Service Desk Manager e offrono in questo modo un singolo repository per tutti gli incidenti nell'ambiente di supporto.

Per creare un ticket in SAP

1. Accedere a SAP Solution Manager.
2. Eseguire una transazione che includa il menu Help (?).
Creare un ticket dal menu.
3. Scegliere Help (?), Create Support Message (Crea messaggio supporto) dal menu File.
Viene visualizzata la pagina Create Message (Crea messaggio).
4. Procedere come segue:
 - Immettere una descrizione breve.
 - Selezionare una priorità per il ticket.
 - Immettere una descrizione lunga.
5. Fare clic sull'icona della posta per inviare il ticket, come illustrato nell'esempio seguente:

Un messaggio conferma la creazione del ticket e assegna un numero di richiesta.

Come tenere traccia degli incidenti SAP in CA Service Desk Manager

Al termine dell'integrazione, testare le comunicazioni in uscita da SAP Solution Manager a CA Service Desk Manager per tenere traccia degli incidenti avviati da SAP in CA Service Desk Manager.

Per tenere traccia degli incidenti SAP

1. Creare un messaggio di supporto da qualsiasi interfaccia client SAP scegliendo Help (?), Create Support Message (Crea messaggio di supporto) dal menu File.
2. Inviare il ticket.

Un messaggio conferma la corretta creazione del messaggio di supporto in SAP.

3. Eseguire la transazione `/nCRMD_ORDER`.

Viene visualizzata la pagina Search for Business Transactions (Cerca transazioni aziendali).

4. Fare clic sulla scheda Find (Trova), selezionare Service (Servizio) dall'elenco a discesa Find (Trova) e fare clic su Start (Avvia).

Vengono visualizzati i risultati della ricerca.

5. Fare doppio clic sul messaggio e selezionare Edit (Modifica).

6. Aggiungere un valore valido per la parte acquirente, il supporto tecnico e qualsiasi altro valore desiderato, finché non saranno presenti flag rossi nel messaggio salvato.

7. Fare clic su Action (Azione) e selezionare Synchronize with CA Service Desk Manager (Sincronizza con CA Service Desk Manager).

8. Salvare di nuovo il messaggio.

Nell'ultima scheda del messaggio SAP viene visualizzato il numero di incidente CA Service Desk Manager risultante.

Nota: la prima volta che si sincronizza un incidente con CA Service Desk Manager potrebbe essere necessario compilare inizialmente SAP.

9. Selezionare la scheda Transaction Data (Dati transazione).

10. Selezionare la scheda Documents (Documenti), come illustrato nell'esempio seguente:

Viene visualizzato l'incidente risultante in CA Service Desk Manager.

Nell'esempio seguente viene mostrata la scheda SAP nella pagina Dettagli incidente di CA Service Desk Manager:

Creazione di un ticket CA Service Desk Manager che viene propagato a SAP Solution Manager

Dopo l'integrazione di CA Service Desk Manager con SAP Solution Manager, è possibile testare la connessione creando un incidente di CA Service Desk Manager che viene propagato a SAP Solution Manager.

Per creare l'incidente

1. Accedere a CA Service Desk Manager.
2. Nella scheda Service Desk, selezionare File, Nuovo incidente.

Viene visualizzata la pagina Crea nuovo incidente.

3. Compilare i campi appropriati per il ticket assicurandosi di assegnare come Area incidente l'area Accesso SAP [creata in precedenza](#) (a pagina 606).
4. Salvare e inviare l'incidente.

L'incidente viene salvato e propagato a SAP Solution Manager.

Visualizzazione di una richiesta CA Service Desk Manager

Utilizzare Fast Entry (Immissione rapida) per visualizzare o aggiornare gli attributi critici di una richiesta service desk di SAP Solution Manager. La scheda Transactional Data (Dati transazionali) consente di aggiornare i dettagli della richiesta. Per impostazione predefinita, viene visualizzata l'ultima transazione visualizzata o creata.

Per visualizzare una richiesta CA Service Desk Manager

1. Eseguire la transazione `/nCMRD_ORDER`.

Per impostazione predefinita, viene aperta l'ultima richiesta visualizzata o creata.

Importante Se nel messaggio di supporto viene visualizzato un flag rosso, fare clic sull'icona di modifica e aggiungere un valore valido per la parte acquirente, il supporto tecnico e qualsiasi altro valore da aggiungere. Aggiungere valori finché non saranno presenti flag rossi nel messaggio salvato.

Nella schermata seguente vengono illustrati l'icona di modifica e il flag rosso del messaggio di supporto:

2. Se si desidera visualizzare un'altra richiesta, fare clic su Business Transaction (Transazione aziendale), Open Business Transaction (Apri transazione aziendale).

Viene visualizzata la pagina di modifica del messaggio di supporto.

3. Selezionare la scheda Transaction Data (Dati transazione).
4. Selezionare la scheda Overview (Informazioni generali).

Nella pagina di modifica del messaggio di supporto vengono visualizzate le informazioni dettagliate e la cronologia della richiesta, come illustrato nell'esempio seguente:

5. (Facoltativo) È possibile attivare manualmente la creazione o l'aggiornamento di un messaggio da SAP Solution Manager a CA Service Desk Manager selezionando Actions (Azioni), Synchronize with CA Service Desk Manager (Sincronizza con CA Service Desk Manager).

Nell'esempio seguente viene mostrato come sincronizzare il ticket con CA Service Desk Manager:

6. (Facoltativo) Nella scheda Transaction Data (Dati transazione) selezionare l'ultima scheda Documents (Documenti).

Viene visualizzato il collegamento tra la richiesta di SAP Solution Manager e CA Service Desk Manager.

Visualizzazione del registro applicazione di sistema

L'applicazione di sistema SAP registra tutte le interazioni con i servizi Web prodotte dall'integrazione con CA Service Desk Manager. Le voci del registro vengono rimosse dopo 14 giorni.

Per esaminare il registro applicazione di sistema

1. Eseguire la transazione */nSLG1*.
Viene visualizzato il registro Analyze Application (Analizza applicazione).
2. Per visualizzare registri specifici di CA Service Desk Manager, effettuare le operazioni seguenti:
 - a. Immettere **/CASD/LOG** nel campo Object (Oggetto).
 - b. Selezionare *All Logs* (Tutti i registri) in Log Class (Classe registro).
 - c. Selezionare *Qualsiasi* in Log Creation (Creazione registro).
 - d. Selezionare *Format Completely from Database* (Formatta completamente dal database) in Log Source and Formatting (Origine registro e formattazione).
3. Fare clic sull'icona di esecuzione .
Viene visualizzata la pagina Display Logs (Visualizza registri) con i risultati della ricerca.
4. Selezionare una voce di registro nell'elenco.
Vengono visualizzati i dettagli del registro, come nell'esempio seguente:

Mantenimento dei dati di tabella in SAP Solution Manager

I dati di tabella vengono mantenuti per confermare l'impostazione dei valori corretti nelle tabelle dei riferimenti incrociati.

Per mantenere i dati di tabella

1. Eseguire la transazione */nSM30*.

Viene visualizzata la schermata Maintain Table View: Initial (Mantieni vista tabella: Iniziale).

2. Immettere **/casd/map_pri** nel campo Table/View (Tabella/Vista) e premere Invio.

Viene visualizzata la pagina Data Browser: Table /CASD/MAP_PRI (Browser dati: Tabella /CASD/MAP_PRI) con i valori della tabella /CASD/MAP_PRI, come nell'esempio seguente:

3. (Facoltativo) Selezionare una riga per modificare la tabella in base all'ambiente corrente.

I dati di tabella vengono mantenuti e confermano che i valori impostati nelle tabelle dei riferimenti incrociati sono corretti.

Messaggi definiti dall'integrazione con CA

Se si ricevono errori specifici di CA durante l'integrazione, fare riferimento all'elenco seguente di codici di errore e messaggi definiti:

000	Messaggio di prova: &1 &2 &3 &4
001	CA WService sapCreateRequest chiamato: Numero esterno &1
002	CA WService sapCreateRequest riuscito: Richiesta &1 creata
003	Errore CA WService sapCreateRequest: Nessuna richiesta ha creato il numero esterno &1
004	Errore servizio Web CA WService sapCreateRequest: Codice di errore &1 &2 &3 &4
011	CA WService sapCreateActivityLog chiamato: Numero richiesta &1
012	CA WService sapCreateActivityLog riuscito: Richiesta &1 aggiornata
013	Errore CA WService sapCreateActivityLog: Aggiornamento richiesta &1 non riuscito
021	CA WService sapCloseIncident chiamato: Numero richiesta &1
022	CA WService sapCloseIncident riuscito: Richiesta &1 chiusa

- 023 Errore CA WService sapCloseIncident: Chiusura richiesta &1 non riuscita
- 031 Chiamata a CA WService Outbound CreateRequest: Numero richiesta &1
- 032 Errore CA WService Outbound CreateRequest: &1
- 036 Chiamata a CA WService Outbound CreateSendSolution: Numero richiesta &1
- 037 Errore CA WService Outbound CreateSendSolution: &1
- 041 Chiamata a CA WService Outbound CreateActivityLog: Numero richiesta &1
- 042 Errore CA WService Outbound CreateActivityLog: &1
- 046 Chiamata a CA WService Outbound ChangeStatus: Numero richiesta &1
- 047 Errore CA WService Outbound ChangeStatus: &1
- 051 Chiamata a CA WService Outbound CloseIncident: Numero richiesta &1
- 052 Errore CA WService Outbound CloseIncident: &1
- 055 Chiamata a CA WService Outbound UpdateObject: Numero richiesta &1
- 056 Errore CA WService Outbound UpdateObject: &1
- 060 Contatto per &1 trovato in CA Service Desk GUID &2.
- 061 Contatto per &1 creato in CA Service Desk GUID &2.
- 062 Contatto per &1 NON creato correttamente in CA Service Desk.
- 070 Incidente tabella /CASD/XREF_REQ aggiornato correttamente: &1
- 071 Errore di aggiornamento incidente tabella /CASD/XREF_REQ: &1
- 072 Duplicato trovato durante aggiornamento incidente tabella /CASD/XREF_REQ: &1
- 073 Flag di chiusura aggiornato correttamente per incidente tabella /CASD/XREF_REQ: &1
- 074 Errore di aggiornamento flag di chiusura per incidente tabella /CASD/XREF_REQ: &1
- 100 Ricerca priorità non riuscita per valore priorità &1. Valore medio predefinito
- 101 Handle di accesso riuscito a CA Service Desk &1.
- 102 Replica messaggio ignorata. Nessun ID agente assegnato.

- 103 Accesso a CA Service Desk non riuscito: &1
- 104 È necessario mantenere nome utente e password CA nella tabella /CASD/AUTH
- 100 Ricerca priorità non riuscita per valore priorità &1. Valore medio predefinito
- 101 Handle di accesso riuscito a CA Service Desk &1.
- 102 Replica messaggio ignorata. Nessun ID agente assegnato.
- 103 Accesso a CA Service Desk non riuscito: &1
- 104 È necessario mantenere nome utente e password CA nella tabella /CASD/AUTH
- 901 Il nome utente non può essere vuoto.
- 902 La password non può essere vuota.
- 903 Errore di crittografia funzione /CASD/SERVICEDESK_ENCRYPT_TEXT. Chiusura programma
- 904 Errore di decrittografia funzione /CASD/SERVICEDESK_DECRYPT_TEXT. Chiusura programma

Codici di eccezione restituiti da SAP Solution Manager a CA Service Desk Manager

Se si ricevono errori specifici di SAP durante l'integrazione, fare riferimento all'elenco seguente di codici di eccezione restituiti:

- 001-009 - Chiamate non valide del sistema esterno
 - 009 Chiamata generica non valida
 - 001 Nessun GUID incidente
 - 002 Nessun GUID richiedente
 - 003 Nessun GUID provider
 - 004 Il GUID del richiedente e il GUID del provider sono uguali
- 010-019 - Chiamata rifiutata dal sistema esterno
 - 010 Rifiuto generico
 - 012 Autorità mancante
 - 011 Incidente bloccato
 - 013 ID sistema esterno sconosciuto
 - 014 ID incidente sconosciuto

- 090-098 - Si è verificato un errore interno imprevisto
 - 090 Errore interno generico
 - 99 - Errore non specificato generalmente causato dall'esecuzione errata di /nICTCONF.

Appendice A: Directory degli esempi

Questa sezione contiene i seguenti argomenti:

[Contenuto della directory degli esempi](#) (a pagina 615)

Contenuto della directory degli esempi

È possibile modificare diversi file nella directory \$NX_ROOT/samples da utilizzare con varie interfacce esterne. Tali file sono raggruppati in diverse sottodirectory. Nessuno dei file presenti nella directory degli esempi è eseguibile nel formato originale.

asset

assetx.sch

Questo file definisce il minimo necessario per una tabella di estensione asset.

assetx.maj

Questo file è una tabella di estensione di esempio.

assetx.spl

Questo file illustra come definire il metodo richiesto per la copia di un asset.

myco_demo.caz

Questo file contiene una visualizzazione dei processi aziendali di esempio.

Modalità di modifica del catalogo dei messaggi

Per modificare il catalogo dei messaggi, completare i passaggi seguenti:

1. Fare riferimento al formato del file `f pdm.xml` contenuto in `$nx_root\bin`.
2. Creare una copia personalizzata di `pdm.xml` e inserirla nella directory `$nx_root\msg_catalog`.
3. Aggiungere, modificare o aggiungere e modificare i messaggi nei file di messaggi XML del passaggio precedente.

macro_lock

Questo file contiene un frammento spel che può essere eseguito utilizzando un bop_cmd per disattivare i blocchi impostati dalle macro.

ntf_meth

Questi sono esempi di metodi di notifica. Come già indicato, potrebbe essere necessario apportare delle modifiche prima di utilizzarli con il sistema in uso. Questi script devono essere eseguiti con un interprete della shell Bourne.

Nota: in UNIX questi script vengono eseguiti nel modo in cui sono scritti. Tuttavia, su Windows NT, è necessario che un interprete shell Bourne di terzi venga installato sul server o che gli script vengano riscritti come file .bat o file c compilati. È possibile anche installare un interprete Perl e convertire gli script in formato Perl.

hp.pdm_pager0 (solo UNIX)

hp.pdm_pager1 (solo UNIX)

hp.sendpage0 (solo UNIX)

hp.sendpage1 (solo UNIX)

pager.p (solo UNIX)

sun.pdm_pagera (solo UNIX)

sun.pdm_pagerb (solo UNIX)

sun.sendpagea (solo UNIX)

sun.sendpageb (solo UNIX)

Questi file contengono metodi di notifica di esempio per i cercapersone che potrebbero non funzionare con cercapersone diversi.

pager_notify.pl

Questo file contiene uno script Perl di esempio che è possibile modificare e utilizzare come metodo di notifica per i cercapersone.

Nota: si tratta solo di un esempio che potrebbe non funzionare con cercapersone diversi.

pdmconf

web.xml.tpl

pdm_startup.tpl

pdm_edit_usage_notes.htm

alias_install.bat

web.cfg.tpl

pdm_startup.i.tpl

pdm_edit.pl

README_files

Tutti questi file vengono utilizzati da pdm_edit.pl per creare file di avvio per un server primario e dei server secondari configurati per l'esecuzione di una serie di daemon.

call_mgt

Contiene esempi per la personalizzazione in Gestione richieste.

gencr.frg

Questo file può essere utilizzato con bop_cmd per creare richieste da una riga di comando. Vengono attivate tutte le notifiche e le voci del registro attività, sebbene non vi sia alcun modulo di richiesta visualizzato sul server al momento della creazione. È necessario utilizzare il parametro -ud per eseguire gencr.frg con l'utilità bob_cmd. Leggere il file gencr_readme.txt per conoscere la sintassi e come modificarla, se necessario. Il file dovrebbe trovarsi nella directory \$NX_ROOT/site/mods/interp; se la directory non esiste, è necessario crearla. Esempio: bop_cmd -d domsrvr -u nsm -f gencr.frg "gencr('My Description')"

iss_site.mod

Questo file può essere utilizzato per attivare la registrazione delle attività dei campi adattati al sito nelle questioni. Questo file dovrebbe trovarsi in \$NX_ROOT/site/mods/majic dopo che è stato modificato per i campi adattati al sito.

cr_site.mod

Questo file può essere utilizzato per attivare la registrazione delle attività dei campi adattati al sito nelle richieste. Questo file dovrebbe trovarsi in \$NX_ROOT/site/mods/majic dopo che è stato modificato per i campi adattati al sito.

chg_site.mod

Questo file può essere utilizzato per attivare la registrazione delle attività dei campi adattati al sito negli ordini di cambiamento. Questo file dovrebbe trovarsi in \$NX_ROOT/site/mods/majic dopo che è stato modificato per i campi adattati al sito.

gencr_readme.txt

Questo file contiene le istruzioni su come utilizzare il file gencr.frg.

chg_site.spl

Questo file può essere modificato per apportare modifiche all'associazione degli attributi al momento della creazione di un ordine di cambiamento da una richiesta. Questo file dovrebbe trovarsi in \$NX_ROOT/site/mods/majic dopo aver apportato le modifiche appropriate.

audlog_site.mod

Questo file può essere utilizzato per attivare il registro di controllo dei campi adattati al sito. Questo file dovrebbe trovarsi in \$NX_ROOT/site/mods/majic dopo che è stato modificato per i campi adattati al sito.

Notify_add.spl (solo UNIX)

Questo file può essere utilizzato per aggiungere l'agente di registrazione, l'assegnatario e il gruppo della richiesta all'elenco delle notifiche di richiesta. Questo file dovrebbe trovarsi in \$NX_ROOT/site/mods/majic.

Notify_replace.spl (solo UNIX)

Questo file può essere utilizzato per aggiungere l'agente di registrazione, l'assegnatario e il gruppo della richiesta all'elenco delle notifiche di richiesta quando vengono modificati. Questo file dovrebbe trovarsi in \$NX_ROOT/site/mods/majic.

sdk

Questa directory contiene un file di esempio per effettuare chiamate dei servizi Web CA Service Desk Manager.

Nel file TableOfContents.doc viene ulteriormente illustrato il contenuto disponibile. Tale file si trova nella directory seguente:

\$NX_ROOT\samples\sdk\websvc

Nei file PKI_loginServiceManaged_JAVA_steps.doc e PKI_loginServiceManaged_PERL_steps.doc viene descritto come configurare ServiceDesk per gli accessi tramite certificato digitale. Tali file si trovano nella directory seguente:

\$NX_ROOT\samples\sdk\websvc\java\test1_pki

Di seguito sono elencati esempi di codice PERL e JAVA con le relative posizioni:

Esempi PERL

`$NX_ROOT\samples\sdk\websvc\perl\test1_pki`

Esempio: chiamata al servizio Web `loginServiceManaged()`

Esempi JAVA

`$NX_ROOT\samples\sdk\websvc\java\test1_pki`

Esempio: chiamata ai servizi Web `loginServiceManaged()` e `getBopsid()`

`$NX_ROOT\samples\sdk\websvc\java\test2_basic`

Esempio: chiamata combinata ai servizi Web `CreateRequest()` e `CreateChangeOrder()`

Appendice B: Caricamento di contenuti aggiuntivi

sd_content.dat

Nel file `sd_content.dat` si trovano contenuti aggiuntivi per CA Service Desk Manager. Questo file di dati contiene i record di categorie di cambiamento e cause principali. Per caricare i dati da una finestra di comando, accedere alla directory `$NX_ROOT/data` ed eseguire questo comando:

```
pdm_load -f sd_content.dat
```