CA Identity Manager

Note di rilascio

r12

Riferimenti ai prodotti CA

La presente documentazione fa riferimento ai seguenti prodotti CA:

- CA Identity Manager
- CA SiteMinder® Web Access Manager
- CA Security Command Center (SCC)
- CA Audit
- eTrust® Directory (denominato anche CA Directory)

Come contattare il servizio clienti

Per l'assistenza tecnica in linea e per un elenco completo delle località, degli orari in cui il servizio è attivo e dei numeri di telefono, contattare il servizio clienti all'indirizzo http://www.ca.com/worldwide.

Sommario

Capitolo 1: Introduzione

Nel presente documento sono contenute informazioni relative ai sistemi operativi supportati, all'installazione del prodotto, ai problemi noti e a come contattare il Supporto tecnico CA.

Capitolo 2: Nuove funzioni

Questa sezione contiene i seguenti argomenti:

Piattaforme e versioni supportate

In Identity Manager r12, sono state aggiunte versioni del server di applicazione, directory e database supportati.

Nota: per un elenco completo delle piattaforme e versioni supportate, vedere la matrice di supporto di Identity Manager nel sito del supporto di Identity Manager http://ca.com/support.

Architettura di Identity Manager

L'architettura di Identity Manager r12 comprende le modifiche riportate di seguito rispetto alle versioni precedenti:

- **Server di fornitura e Gestione fornitura incorporati**

  Il server di fornitura è il server con cui vengono gestiti gli account aggiuntivi assegnati ad un utente di Identity Manager. Quando si assegna un ruolo di fornitura ad un utente di Identity Manager, sul server di fornitura vengono creati account sugli endpoint che soddisfano i requisiti del ruolo. Ad esempio, se viene assegnato un ruolo di fornitura che include un modello di account Exchange, sul server di fornitura viene assegnato un account Exchange all'utente.

  Gestione fornitura rappresenta l'interfaccia utente per la gestione dei tipi di endpoint, come Exchange oppure Oracle, e degli endpoint stessi, come un sistema specifico su cui è installato Exchange. In precedenza, tale interfaccia era detta eTrust Admin Manager. In Gestione fornitura sono disponibili altre funzionalità, come l'esplorazione e la correlazione di account; tuttavia, tali funzionalità aggiuntive sono ora duplicate nella console utente di Identity Manager, da dove risultano più facilmente accessibili.

  Per la fornitura, nelle versioni precedenti di Identity Manager era necessario eTrust Admin.

  Nota: Server di fornitura e Gestione fornitura sono componenti aggiuntivi.

- **Integrazione di Identity Manager con SiteMinder**

  SiteMinder non è più un prerequisito per l'installazione di Identity Manager. Ora l'integrazione con SiteMinder è facoltativa e consente di ottenere funzionalità avanzate, tra cui l'autenticazione SiteMinder e Criteri password avanzati.

  Per le funzionalità seguenti, nelle versioni precedenti di Identity Manager era necessario SiteMinder:

  – Autenticazione

  – Archiviazione di informazioni su ruoli e attività (nell'archivio dei criteri)

  – Collegamento ad un archivio utenti

  – Criteri password

  In Identity Manager, questa funzionalità viene fornita in modo nativo.

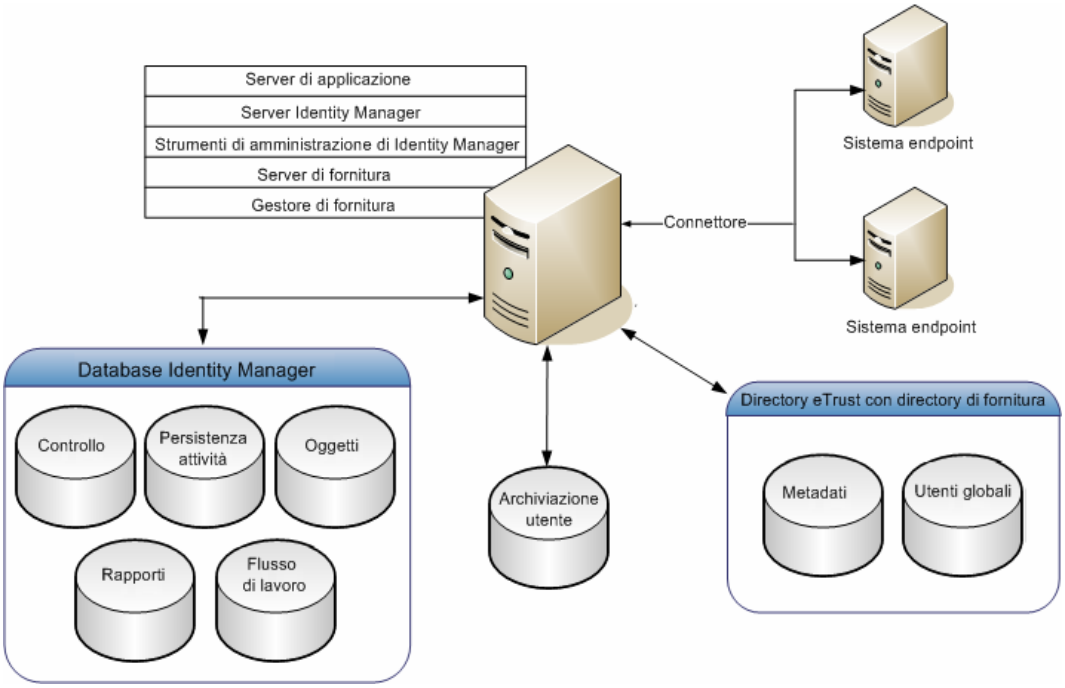
  Nota: l'integrazione con SiteMinder consente di ottenere funzionalità avanzate, tra cui l'autenticazione SiteMinder e Criteri password avanzati.

- **Archivio oggetti**

  In Identity Manager r12 le informazioni su ruoli e attività vengono ora archiviate in un nuovo archivio oggetti. L'archivio oggetti è un database relazionale configurato automaticamente da Identity Manager durante il runtime.

La figura seguente mostra un'implementazione di Identity Manager che include la fornitura.

Nota: la directory di fornitura, in cui sono archiviate le informazioni necessarie per utilizzare la fornitura e quelle relative agli utenti globali, deve essere installata nella directory eTrust, prerequisito per l'installazione di Identity Manager con fornitura.



Miglioramenti al programma di installazione

Tutti i componenti necessari per l'installazione server di Identity Manager vengono ora installati mediante un unico programma, compresi i componenti per la fornitura e le estensioni per un server di policy SiteMinder.

Il programma di installazione di Identity Manager comprende il server di fornitura per Identity Manager, la directory di fornitura e gestione fornitura. Consente inoltre di configurare le connessioni ai database contenenti gli archivi dei dati degli oggetti e dei dati per il flusso di lavoro, la persistenza delle attività, i rapporti e il controllo.

Le modifiche apportate all'installazione di Identity Manager comprendono quanto riportato di seguito.

- Per l'autenticazione in Identity Manager non è più necessario SiteMinder.
- La persistenza delle attività non è più facoltativa e viene attivata in fase di installazione.
- Uno schema del database viene esteso automaticamente per ogni database utilizzato da Identity Manager.
- Gli Strumenti di amministrazione sono ora installati nelle posizioni seguenti:
  - **Windows:** C:\Programmi\CA\IAM Suite\Identity Manager\tools
  - **UNIX:** *HOME*/CA/IAM_Suite/Identity_Manager/tools
- Non sono più necessari script post-installazione.

Miglioramenti ai rapporti

I rapporti di Identity Manager consentono di rilevare lo stato attuale di un ambiente di Identity Manager. È possibile utilizzare tali informazioni per garantire conformità con criteri aziendali interni o con normative esterne.

Identity Manager r12 include i miglioramenti dei rapporti riportati di seguito.

- **Integrazione con il server dei rapporti IAM.**

  Identity Manager r12 utilizza Business Objects Enterprise XI per progettare, gestire e visualizzare rapporti dal relativo database. Identity Manager fornisce una versione di runtime di Business Objects e non richiede pertanto una licenza a parte.

- **Nuove attività di amministrazione per l'esportazione dei dati nel database dei rapporti.**

  Identity Manager include nuove attività predefinite, che consentono di esportare dati da Identity Manager al database dei rapporti. Ogni volta che vengono esportati dati al database dei rapporti, viene creata una *snapshot*, una rappresentazione dello stato attuale degli oggetti specificati dall'utente in un ambiente di Identity Manager.

  Mediante le nuove attività predefinite, è possibile creare definizioni di snapshot e acquisire una snapshot da cui generare un rapporto.

- **Rapporti predefiniti aggiuntivi**

  Identity Manager include i rapporti predefiniti riportati di seguito, utilizzabili senza modificarli o personalizzandoli in base alle proprie esigenze aziendali.

  - **Account endpoint**

    Elenco di account per nome account, proprietario e data ora di creazione per ogni endpoint, ordinati per tipo di endpoint.

  - **Account non standard**

    Elenco degli account non standard, quali account orfani e di sistema.

  - **Tendenze degli account non standard**

    Tendenze degli account non standard, per tipo di account non standard, visualizzate sotto forma di grafici.

  - **Account orfani**

    Elenco degli account che non sono associati con un utente. Gli account orfani sono elencati per nome account, proprietario e data ora di creazione per ogni endpoint e ordinati per tipo di endpoint.

  - **Criteri**

    Elenco di criteri, comprese le relative condizioni, e azioni Azione su Applica e Azione su Rimuovi.

  - **Amministratori di ruolo**

    Elenco degli amministratori di ruolo.

  - **Membri di ruolo**

    Elenco dei membri di ruolo.

  - **Proprietari di ruolo**

    Elenco di proprietari di ruolo.

  - **Ruoli**

    Elenco dei ruoli e relative descrizioni.

  - **Snapshot**

    Elenco di tutte le snapshot disponibili nel database dei rapporti.

  - **Ruoli attività**

    Elenco delle attività per descrizione, categoria e tipo. Per ogni attività, specificare tutti i ruoli associati.

  - **Account utente**

    Elenco degli account per utente. Gli account utente sono elencati per nome account, attributi account ed endpoint, ordinati per tipo di endpoint.

- **Stato di sincronizzazione del criterio utente**

  Elenco di utenti, comprensivo dei criteri attualmente allocati e di quelli da riallocare.

- **Profilo utente**

  Elenco di utenti con tutte le informazioni disponibili su di essi.

- **Diritti utente**

  Elenco di utenti e degli account, dei ruoli e dei gruppi associati.

Gestione della connessione

Gestione della connessione consente di configurare i dettagli della connessione al server di database in Identity Manager. Quando in Identity Manager è necessario eseguire la connessione ad un server di database, a tale scopo vengono utilizzati i dettagli di Connessione. Gestione della connessione consente di creare più connessioni a diversi server di database in un Tipo di connessione. Per ogni Tipo di connessione è possibile specificare una connessione predefinita. È necessario configurare un Tipo di connessione primario per Identity Manager mediante la console di gestione.

Miglioramenti alla fornitura

Con questa release, sono disponibili più azioni da eseguire nella console utente di Identity Manager. Alcune di queste funzionalità in precedenza erano disponibili in eTrust Admin Manager. La console utente consente di eseguire le operazioni riportate di seguito.

- Esplorare e mettere in correlazione account sugli endpoint.
- Mettere in correlazione account orfani e di sistema con un utente di Identity Manager.
- Verificare le azioni di fornitura, come l'assegnazione di un ruolo di fornitura ad un utente globale.

Inoltre, questa release comprende:

- Connector Xpress, uno strumento grafico per la creazione di connettori personalizzati.
- Supporto per connettori dinamici (JNDI e JDBC) da utilizzare con i metadati XML generati da Connector Xpress.
- Server di connessione Java, un server che gestisce le richieste dei connettori Java.
- Funzioni di alta disponibilità per il server di connessione C++, precedentemente noto come Super Agente.

- Nuovi connettori Java per Kerberos, per amministrare i principali Kerberos e i criteri password Kerberos su server Solaris.
- Nuovi connettori Java per SAP (con supporto CUA).
- Nuovi connettori Java per Oracle, MS-SQL e 0S/400, forniti con il server di connessione Java.

  Questi tre connettori sostituiscono le opzioni di esempio, che non sono più supportate.
- Miglioramenti a Gestione fornitura, per fornire un'interfaccia utente generica per tipi di endpoint JDBC e JNDI dinamici creati con Connector Xpress.

GUI DYN

L'interfaccia GUI DYN è stata ottimizzata in Gestione fornitura per offrire un set ottimizzato di funzioni, il quale consente di manipolare gli oggetti endpoint arbitrari, con un solo plug-in di Gestione fornitura.

Ad esempio, quando si esegue la mappatura di un campo in Connector Xpress, viene posizionato un elemento nei metadati, il quale rappresenta un campo. Quando si esamina un qualsiasi oggetto nel suddetto connettore, l'interfaccia GUI DYN utilizza i metadati per visualizzare i campi appropriati.

Le modifiche in questa versione ampliano le funzionalità dell'interfaccia GUI DYN, grazie al set ottimizzato di funzioni, rendendo in tal modo più semplice un'eventuale, futura aggiunta di nuove funzioni, ottimizzando allo stesso tempo la visualizzazione per l'utente.

Connettore Lotus Notes/Domino rilasciato come anteprima tecnica

Per la versione r12 di Identity Manager, il connettore LND basato su Java viene rilasciato solo come anteprima tecnica.

Questo connettore **non** dispone della certificazione per gli ambienti di produzione. Il connettore con certificazione completa sarà disponibile in una versione CR. Per ulteriori informazioni, contattare il responsabile account.

Nota: non installare il connettore LND C++ e il connettore LND Java nello stesso ambiente Identity Manager.

Miglioramenti alla generazione di rapporti di stato

Identity Manager r12 include diverse funzioni che consentono di consultare lo stato delle attività.

Miglioramenti a Visualizza attività inoltrate

Identity Manager r12 include la scheda Visualizza attività inoltrate, che consente di visualizzare lo stato di un'attività, la sua dipendenza da altre attività, eventi e flusso di lavoro.

In Identity Manager r12, alla scheda Visualizza attività inoltrate sono stati apportati i miglioramenti descritti di seguito.

- Nella scheda Visualizza attività inoltrate sono ora visualizzati più dettagli sulle attività e gli eventi associati.
- Nella scheda Visualizza attività inoltrate è possibile annullare le attività in sospeso e ripetere l'inoltro o rifiutare le attività non riuscite.
- Ora è possibile configurare la scheda Visualizza attività inoltrate.

Attività Visualizza attività utente

L'attività utente è una cronologia delle attività che coinvolgono un utente specifico. Visualizza attività utente consente agli amministratori di tenere traccia delle informazioni utente seguenti:

- Attività eseguite sull'utente.
- Attività eseguite dall'utente.
- Approvazioni del flusso di lavoro eseguite dall'utente.

Come visualizzare l'attività dell'utente

1. Fare clic su Utenti, Gestisci utenti, Visualizza attività utente.

   Verrà visualizzato lo schermo Seleziona utente.

2. Ricercare un utente e fare clic su Seleziona.

   Verrà visualizzato lo schermo Visualizza attività utente.

   Per ulteriori informazioni sull'attività utente visualizzata, consultare la *Guida in linea della Console utente*.

Scheda Cronologia utente

La scheda Cronologia utente consente di visualizzare le attività legate ad un utente. È possibile aggiungerla ad un'attività Modifica utente o Visualizza utente.

Nota: questa scheda è inclusa nell'attività Visualizza attività utente.

I dettagli delle attività visualizzati in questa scheda sono consultabili anche nella scheda Visualizza attività inoltrate.

Miglioramenti al flusso di lavoro

Identity Manager r12 include miglioramenti alle funzionalità del flusso di lavoro che nel semplificano il processo di creazione e aggiungono nuove funzioni. Questi miglioramenti sono descritti nelle sezioni che seguono.

Modelli di processo del flusso di lavoro

I modelli di processo del flusso di lavoro consentono di configurare e gestire completamente il controllo del flusso di lavoro dalla console utente di Identity Manager. Questi modelli di processo generici possono essere configurati per controllare la maggior parte delle attività e degli eventi di Identity Manager.

I nuovi modelli di processo consentono il controllo del flusso di lavoro sia a livello di attività che a livello di evento, semplificano la configurazione dei resolver partecipante per i revisori e i processi di approvazione in più passaggi.

Inoltre, è possibile determinare l'elenco dei revisori in modo dinamico durante il runtime, in base agli attributi dell'attività o dell'evento in corso di approvazione.

Flusso di lavoro a livello di attività

È possibile associare processi del flusso di lavoro sia con attività che con eventi. Ciò significa che i partecipanti possono approvare o rifiutare un'attività di Identity Manager nel suo complesso oppure un evento specifico all'interno di tale attività.

Il flusso di lavoro a livello di attività consente ai partecipanti di rivedere tutti gli eventi prima di decidere se approvare o rifiutare una richiesta. Quando un processo del flusso di lavoro viene associato ad un evento specifico all'interno di un'attività, un revisore non può visualizzare il contesto complessivo dell'attività all'interno del quale è stata presentata una richiesta.

Comandi operazione del flusso di lavoro

È possibile aggiungere nuovi pulsanti alle attività di approvazione del flusso di lavoro, ad integrazione o sostituzione dei pulsanti di Approva e Rifiuta standard. Una dimostrazione di esempio di questa funzione è disponibile nelle attività di richiesta in linea.

Richieste in linea e cronologia

Nella console utente, gli utenti possono richiedere modifiche ai propri account e gli amministratori possono apportare tali modifiche. Queste attività attivano a loro volta un modello di processo del flusso di lavoro che richiede fino a tre revisori: un consulente che commenti la richiesta, un utente aziendale che la approvi e un esperto tecnico che la implementi.

Le attività di richiesta in linea comprendono inoltre un nuovo comando cronologia, che consente ai revisori di aggiungere note o commenti all'attività nelle diverse fasi del suo completamento.

Pianificazione delle attività

La pianificazione consente di posticipare l'esecuzione automatica di un'attività ad una data futura. Se viene pianificata un'attività associata ad un processo del flusso di lavoro, in Identity Manager vengono eseguite tutte le attività definite in tale processo. Lo stato delle attività pianificate è consultabile nella pagina Visualizza attività inoltrate.

Un'attività pianificata non ancora eseguita da Identity Manager può essere ripianificata o annullata utilizzando la pagina Visualizza attività inoltrate.

In Identity Manager è disponibile un'utilità di pianificazione sotto forma di scheda speciale. Per accedere a tale utilità, è necessario configurare un'attività mediante la scheda Pianificazione.

Miglioramenti alla console utente

Identity Manager r12 include numerosi miglioramenti che aggiungono il supporto di nuove funzioni e aumentano la facilità d'uso. Questi miglioramenti sono illustrati nelle sezioni che seguono.

Guida personalizzata

Identity Manager consente di creare elementi di guida personalizzati per attività e schede che sono state personalizzate nella console utente. Per implementare a guida personalizzata, è possibile creare un sistema di guida sensibile al contesto con file di guida HTML personalizzati o pagine Wiki e reindirizzare i collegamenti alla guida nella console utente di Identity Manager per accedere alla guida personalizzata.

Questa funzione consente inoltre di tradurre i file della guida predefiniti, in inglese, in un'altra lingua.

Attività nidificate

Un'attività nidificata è un'attività di amministrazione che può essere aperta da una scheda Profilo associata ad un'altra attività. Gli utenti della prima attività aprono l'attività nidificata facendo clic su un collegamento o un pulsante. Ad esempio, alla scheda Modifica utente è possibile aggiungere un pulsante Elimina utente. Se un account utente non è più valido, un amministratore può fare clic sul pulsante Elimina utente per rimuovere l'account senza dover tornare al riquadro di esplorazione per selezionare una nuova attività.

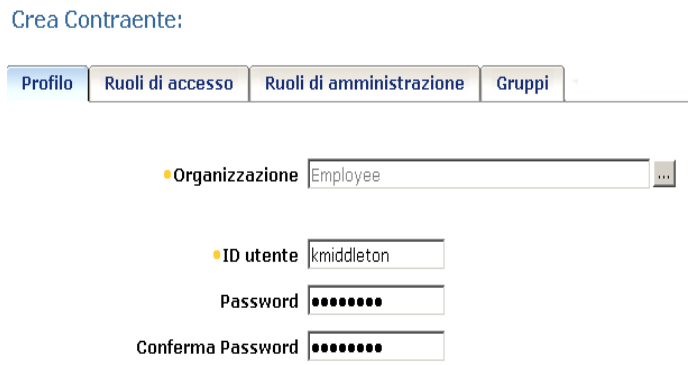
Controller di scheda

Un controller di scheda determina la modalità di visualizzazione delle schede all'interno di un'attività. È possibile selezionare uno dei seguenti controller di scheda:

- **Controller scheda standard**

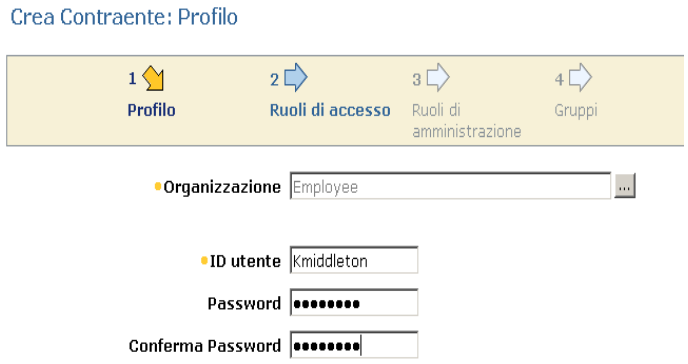
  Visualizza le schede dell'attività in formato di schede indipendenti. Gli utenti possono utilizzare le schede all'interno dell'attività in base ad un ordine qualsiasi.

  Questo è il controller di scheda predefinito.



- **Controller di scheda della procedura guidata**

  Visualizza le schede incluse in un'attività in formato di procedura guidata. Gli amministratori utilizzando ciascuna scheda nell'ordine riportato.



- **Controller scheda di sequenza**

  Visualizza una scheda alla volta. Ogni scheda occupa un riquadro a sé stante. Gli utenti completano una scheda, quindi fanno clic su un pulsante o collegamento personalizzato per passare alla scheda successiva.

  La sequenza di schede, pulsanti e collegamenti visualizzati è determinata a livello del codice JavaScript immesso durante la configurazione del controller di scheda sequenza.

  Nel codice JavaScript personalizzato è possibile specificare l'aspetto e l'ordine delle schede in base all'input dell'utente. Ad esempio, se un utente seleziona un'opzione nella prima scheda, in Identity Manager verrà visualizzata una pagina specifica. Se invece seleziona un'opzione diversa, verrà visualizzata una pagina distinta.

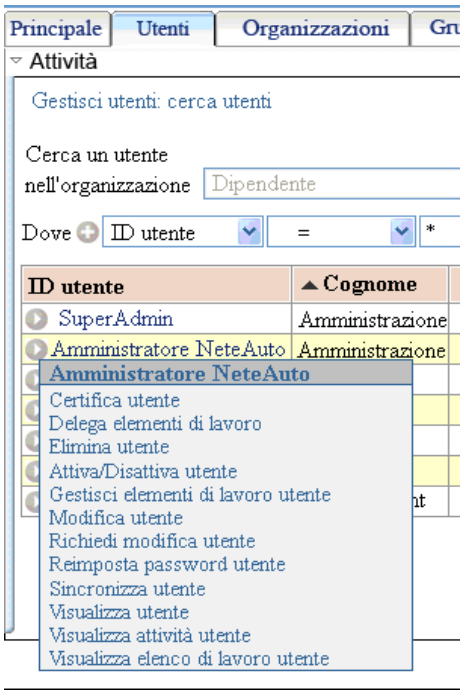
Elenchi di attività

Identity Manager r12 include le nuove attività predefinite riportate di seguito, che consentono di ricercare un oggetto da gestire:

- Gestisci utenti
- Gestisci gruppi
- Gestisci organizzazioni
- Gestisci ruoli di amministrazione
- Gestisci attività di amministrazione
- Gestisci ruoli di accesso
- Gestisci attività di accesso

Dopo aver selezionato l'oggetto, è possibile visualizzare l'elenco delle attività che possono essere utilizzate per gestirlo.

Ad esempio, per modificare un utente con questo metodo, selezionare la categoria Utente, quindi scegliere l'attività Gestisci utente. Cercare e selezionare l'utente che si desidera gestire. Nei risultati della ricerca fare clic su un'icona per visualizzare l'elenco delle attività che è possibile utilizzare per gestire l'utente selezionato. Nell'elenco è possibile selezionare Modifica utente o qualsiasi altra attività appropriata.



È inoltre possibile configurare elenchi di attività in attività diverse da quelle di gestione. Ad esempio, è possibile aggiungere un elenco di attività ad una scheda Appartenenza. In questo caso, sarà disponibile un elenco di attività per ogni membro incluso nella scheda Appartenenza.

Miglioramenti alla scheda Profilo

In Identity Manager r12, la scheda Profilo include una serie di nuove impostazioni di configurazione a supporto delle nuove funzionalità. Queste impostazioni sono descritte nelle sezioni che seguono.

Categorie attività

Le categorie di attività consentono di organizzare le attività in modo da semplificarne l'individuazione e la ricerca nella console utente.

È possibile specificare tre categorie di attività:

- Categoria 1 rappresenta la categoria di attività di livello superiore. Queste categorie vengono visualizzate sotto forma di schede lungo la parte superiore dello schermo.
- Categoria 2 rappresenta la categoria di secondo livello. Questa categoria consente di raggruppare le attività correlate incluse in una categoria di livello superiore. Se non si specifica alcuna categoria di secondo livello, la categoria predefinita è Attività.
- Categoria 3 contiene le attività utilizzate dagli amministratori. Quando gli amministratori fanno clic sul nome della scheda Categoria 3 nella console utente, viene visualizzato l'elenco delle attività incluse in tale categoria.

All'interno di ogni categoria è possibile definire l'ordine in cui vengono visualizzati gli elementi di tale categoria specificando l'ordine desiderato. Ad esempio, nella figura seguente viene mostrata la scheda Dipendente, con l'opzione Ordine categoria impostata su 3.

Nota: se una categoria include più attività, l'ordine della categoria specificato nel profilo per ogni attività deve essere impostato sullo stesso valore. Se l'ordine della categoria è diverso, verranno visualizzate più istanze della scheda della stessa scheda. Si supponga, ad esempio, che la categoria Dipendente contenga due attività, ovvero Crea dipendente e Modifica dipendente. Se l'opzione Ordine categoria per l'attività Crea dipendente è impostata su 3 mentre la stessa opzione per l'attività Modifica dipendente è impostata su 6, la categoria Dipendente verrà visualizzata sotto forma di due schede.

Priorità di attività

In Identity Manager r12, è ora possibile specificare una priorità di attività per garantire che le attività più urgenti vengano eseguite per prime.

Nella scheda Profilo relativa all'attività, è possibile impostare una priorità Alta, Media o Bassa. La priorità predefinita è Media.

Nota: è possibile utilizzare l'attività Visualizza attività inoltrate per cercare attività associate ad una priorità specifica, quindi visualizzarne lo stato.

Dati personalizzati per le caselle di selezione

Gli schermi delle attività di Identity Manager includono campi che consentono agli utenti di selezionare un valore. Questi campi comprendono:

- Casella di controllo selezione multipla
- Casella a discesa
- Casella combinata a discesa
- Selezione multipla
- Selettore opzione

- Casella combinata selettore opzione
- Pulsante di opzione selezione singola
- Selezione singola.

È possibile specificare dati personalizzati da utilizzare per popolare le caselle di selezione nei file XML. Ad esempio, è possibile utilizzare i file XML Dati casella di selezione per popolare le opzioni di una casella a discesa Città o Stato su una scheda Profilo per l'attività Crea utente.

Inoltre, è possibile utilizzare il file XML Dati casella di selezione per configurare una dipendenza tra due campi nello schermo di un'attività. Ad esempio, le opzioni disponibili nel campo Città possono dipendere dall'opzione scelta dall'utente nel campo Stato.

Controllo Selezione data

La console utente di Identity Manager include ora uno stile Selezione data applicabile ai campi su una scheda Profilo per la raccolta e la visualizzazione di date.

Quando viene applicato lo stile Selezione data, accanto ad un campo data viene visualizzata un'icona calendario. Facendo clic sull'icona del calendario, gli utenti possono visualizzare un controllo Calendario, che consente di selezionare la data desiderata.

Controlli Binario e Immagine

Ora è possibile configurare Identity Manager per visualizzare un'immagine su un profilo o includere un attributo binario. Ad esempio, è possibile configurare lo schermo di un profilo utente per visualizzare una fotografia digitale dell'utente gestito o allegare un documento allo schermo del profilo.

Nota: questa funzione è supportata solo per archivi utenti LDAP.

Attributi personalizzati definiti dall'utente per i ruoli

Identity Manager supporta attributi personalizzati definiti dall'utente che consentono di filtrare in modo efficace i ruoli dell'organizzazione. Ad esempio, in un ambiente aziendale potrebbe essere necessario creare più di un centinaio di ruoli diversi. È possibile suddividere tali ruoli in categorie, ad esempio per unità aziendale o per area geografica. Per cercare i ruoli specifici di una particolare area geografica, è possibile utilizzare gli attributi personalizzati per filtrare i ruoli disponibili nell'organizzazione.

È possibile utilizzare gli attributi personalizzati nelle attività di creazione, modifica e visualizzazione per i seguenti ruoli:

- Ruoli di accesso
- Ruoli di amministrazione

È necessario eseguire le seguenti operazioni per aggiungere gli attributi personalizzati alle attività di amministrazione e agli schermi di ricerca.

1. Aggiungere gli attributi personalizzati a qualsiasi attività di amministrazione definita per i ruoli.
2. Configurare gli schermi di ricerca per i ruoli mediante gli attributi personalizzati.

Bulk Loader

La scheda Bulk Loader della console utente consente di caricare file alimentatore utilizzati per manipolare un gran numero di oggetti gestiti simultaneamente. Ad esempio, è possibile creare 1000 utenti in Identity Manager manualmente oppure utilizzare Bulk Loader. Il metodo Bulk Loader presenta il vantaggio di consentire l'automazione del processo di manipolazione di un gran numero di oggetti gestiti utilizzando un file di informazioni (alimentatore). Inoltre, è possibile mappare l'attività Bulk Loader su un processo del flusso di lavoro.

Nota: per l'alimentatore è supportato il formato file CSV, ma è possibile creare un feed personalizzato per altri formati.

Ricerca organizzazione predefinita basata sugli utenti

Per semplificare la console utente, in Identity Manager un amministratore può configurare un'organizzazione predefinita per l'attività Crea utente in base all'utente che sta eseguendo l'attività. Quando un utente esegue l'attività Crea utente, l'organizzazione non viene visualizzata nella scheda Crea profilo utente, bensì impostata automaticamente in base all'organizzazione dell'utente.

Come configurare un'organizzazione predefinita in base all'organizzazione dell'utente

1. Nella console utente di Identity Manager scegliere Ruoli e attività, Attività di amministrazione, Modifica attività di amministrazione.
2. Selezionare l'attività Crea utente.
3. Nella scheda Schede fare clic sulla freccia rivolta verso destra accanto a Profilo.
4. Fare clic sui puntini di sospensione (...) per visualizzare l'elenco degli schermi da modificare.
5. Selezionare lo schermo Crea profilo utente, quindi fare clic su Modifica.
6. Ricercare l'Organizzazione e fare clic sulla freccia rivolta verso destra per modificarla.

   Nota: questo campo non è presente negli ambienti privi di Organizzazioni.
7. Impostare lo stile su Nascosto.
8. Nel campo JavaScript predefinito immettere il codice seguente:

```
function defaultValue(blthContext)
{
return blthContext.getAdministrator().getOrg(null).getUniqueName();
}
```

9. Fare clic su Applica.

Supporto del formato IPv6

Durante la configurazione di Identity Manager è possibile immettere indirizzi sia in formato IPv4 che in formato IPv6.

Identity Manager supporta il formato IPv6 nei seguenti sistemi operativi:

- Solaris 8 o versione successiva
- Windows XP SP1 o versione successiva
- Windows 2003 o versione successiva

Ogni server applicazioni è caratterizzato da requisiti JDK specifici:

- Per un server applicazioni JBoss in un sistema Standalone, Identity Manager supporta il formato IPv6 con JDK1.4.2_13 o 1.5 (su Solaris) o JDK1.5 (su Windows).
- Per un cluster JBoss, non è disponibile alcuna versione di JDK valida per il formato IPv6 alla data di rilascio di Identity Manager r12. Se viene rilasciata una versione di JDK valida per IPv6, la matrice di supporto della piattaforma verrà aggiornata.
- Tuttavia, per un cluster JBoss che utilizza uno stack IPv4/IPv6, Identity Manager supporta il formato IPv6 con JDK1.4.2_13 o 1.5 (su Solaris) o JDK1.5 (su Windows).
- I server applicazioni WebLogic e WebSphere includono JDK 1.5, che supporta gli indirizzi IPv6.

Prendere nota delle seguenti considerazioni prima di procedere alla configurazione di un ambiente che supporta IPv6:

- Affinché Identity Manager supporti gli indirizzi IPv6, tali indirizzi devono essere supportati anche da tutti i componenti inclusi nell'implementazione di Identity Manager, compresi il sistema operativo, JDK, i server di directory e i database.
- In caso di integrazione di Identity Manager con SiteMinder, anche il plug-in del server web per il server applicazioni deve supportare IPv6.
- Durante la connessione a SiteMinder o a qualsiasi database da Identity Manager mediante una connessione JDBC, specificare il nome host e non l'indirizzo IP.
- Il server dei rapporti IAM può essere installato in un host dual stack che supporta i formati IPv4 e IPv6, ma le comunicazioni con il server devono avvenire nel formato IPv4.

  Quando nella console di gestione viene configurata una connessione con il server dei rapporti, il nome del server deve essere immesso in formato IPV4.

Certificazione FIPS 140-2

Identity Manager r12 supporta la certificazione FIPS 140-2 *solo* in una nuova installazione. Identity Manager dispone inoltre di uno strumento per le password che consente di fornire una chiave di crittografia FIPS. Lo strumento è disponibile nella seguente directory:

```
<percorso installazione>\PasswordTool
```

Prendere nota delle seguenti considerazioni in caso di attivazione della certificazione FIPS 140-2 per un ambiente Identity Manager:

- Dopo aver attivato il supporto FIPS 140-2 per una distribuzione Identity Manager, non è più possibile disattivarlo. In modo analogo, se si installa Identity Manager senza attivare il supporto FIPS 140-2, non sarà possibile aggiungere il supporto in un secondo momento.
- Se si attiva il supporto FIPS 140-2 in una distribuzione Identity Manager contenente SiteMinder, la versione di SiteMinder deve essere la r12.

Supporto avanzato delle versioni localizzate

La console utente e la Guida in linea della console utente di Identity Manager sono disponibili nelle seguenti lingue:

- Francese
- Coreano
- Giapponese
- Tedesco
- Cinese semplificato
- Spagnolo
- Italiano

Nota: per informazioni sull'utilizzo di Identity Manager in una di queste lingue, consultare la *Guida alla configurazione*.

Ulteriori informazioni:

Installazione di ambienti Identity Manager localizzati (a pagina 39)

Capitolo 3: Modifiche alle funzioni esistenti

Questa sezione contiene i seguenti argomenti:

Agente filtro servlet obsoleto

L'agente filtro servlet è obsoleto in Identity Manager r12. Si consiglia di utilizzare un Agente Web anziché un Agente filtro servlet. Se è già distribuito un Agente filtro servlet in un ambiente di Identity Manager *esistente*, continuerà a funzionare e ad essere supportato.

Miglioramenti alla console di gestione

La console di gestione di Identity Manager include gli schermi nuovi o modificati riportati di seguito.

- Pagina Console utente: consente di configurare le impostazioni generali per una console utente di Identity Manager, compresi icona e titolo, classe di autenticazione e pagina di disconnessione.

  Nota: in Identity Manager, le impostazioni di icona e titolo venivano configurate nella pagina Temi. Le funzionalità di questa pagina sono state trasferite alla pagina Console utente e la pagina Temi è stata eliminata.

- Pagina Ambienti: consente di arrestare e avviare un ambiente di Identity Manager. Non è necessario riavviare il server di applicazione per rendere effettive le modifiche.

- Pagina Fornitura: questa pagina non include più la configurazione della sincronizzazione in entrata. Per configurare la sincronizzazione in entrata, vedere la *Guida alla fornitura*.

- Pagina Persistenza attività: la persistenza delle attività viene ora configurata automaticamente durante l'installazione. Non è più necessario attivarla manualmente. Questa pagina è stata eliminata.

Modifiche ai criteri di password

Dal momento che per le nuove installazioni di Identity Manager r12 non è più richiesto SiteMinder, sono state apportate alcune modifiche alla funzionalità Criteri di password predefinita. Nelle distribuzioni senza integrazione con SiteMinder, Identity Manager consente di creare criteri di password di base per gestire le password degli utenti mediante l'applicazione di regole e restrizioni che disciplinano la scadenza, la composizione e l'utilizzo delle password.

Se Identity Manager viene configurato per l'integrazione con SiteMinder, è possibile creare criteri di password avanzati che consentono di definire regole e restrizioni aggiuntive.

- Filtri di directory
- Scadenza delle password:
  - Traccia degli accessi non riusciti o completati
  - Autenticazione durante l'accesso
  - Scadenza delle password in caso di mancata modifica
  - Inattività delle password
  - Password errata
- Più espressioni regolari
- Restrizioni delle password:
  - Numero minimo di giorni prima del riutilizzo
  - Numero minimo di password prima del riutilizzo
  - Differenza in percentuale dall'ultima password
  - Ignora la sequenza durante l'analisi delle differenze
  - Corrispondenza degli attributi del profilo
  - Corrispondenza con dizionario

Strumento imrexport obsoleto

Le funzionalità dello strumento imrexport sono state integrate nella console utente di Identity Manager. L'attività Acquisisci dati snapshot nella scheda Rapporti offre ora le funzionalità dello strumento imrexport in Identity Manager r12.

Modifiche all'architettura dei connettori z/OS

I connettori z/OS (CA ACF2, CA Top Secret e RACF) sono stati riarchitettati a scopi prestazionali, al fine di utilizzare CA LDAP Server per z/OS anziché CA DSI Server su z/OS.

Qualsiasi opzione del file di configurazione del server di fornitura correlata a CA LDAP Server, ora viene immessa e archiviata su z/OS, quando CA LDAP Server viene installato. Inoltre, le informazioni di connessione relative al server LDAP mainframe ora vengono immesse attraverso il visualizzatore delle attività dell'endpoint di Gestione fornitura.

Funzioni non più supportate

Alcune funzioni eTrust Admin non sono più disponibili su Identity Manager r12. Nel seguente elenco sono riportate le nuove funzioni presenti in Identity Manager r12.

Funzione eTrust Admin	Funzioni Identity Manager
flusso di lavoro avanzato	Flusso di lavoro WorkPoint
Flusso di lavoro precedente	Flusso di lavoro WorkPoint
Interfaccia Web di auto-amministrazione (SAWI)	Self-service di Identity Manager
Interfaccia Web dell'amministrazione delegata (DAWI)	Amministrazione delegata di Identity Manager
IA Manager	Amministrazione delegata e attività self-service di Identity Manager
Creazione di rapporti di eTrust Admin etaReport	Creazione di rapporti di Identity Manager
Opzione di aggiunta PeopleSoft	Bulk Loader
Opzione di aggiunta universale	Bulk Loader
Opzione SAP (versione 4 C++)	Connettore SAP (versione Java)
Opzione MS SQL (versione 4 C++)	Connettore MS SQL (versione Java)
Opzione Oracle (versione C++)	Connettore Oracle (versione Java)
Opzione OS/400	Connettore OS/400 (versione Java)
Opzione portale CleverPath	Nessuna sostituzione

Nota: le versioni esistenti (disponibili su eTrust Admin 8.1 SP2) dell'opzione di aggiunta PeopleSoft e di aggiunta universale continueranno a funzionare su Identity Manager r12.

Capitolo 4: Requisiti di sistema

Per il sistema host del server di Identity Manager sono previsti i seguenti requisiti hardware minimi:

- CPU: processore singolo o doppio, Intel Pentium III (o compatibile) 700-900 MHz, o Sparc Workstation 440MHz
- Memoria: 2 GB
- Spazio su disco disponibile: 1 GB

Nota: per questi requisiti hardware vengono presi in considerazione i requisiti del server di applicazione da installare sul sistema con il server di Identity Manager.

Capitolo 5: Considerazioni sull'installazione

Questa sezione contiene i seguenti argomenti:

Posizione matrici di supporto

Per un elenco completo delle versioni di software supportate, vedere la matrice di supporto di Identity Manager.

Per visualizzare la matrice di supporto

1. Accedere a support.ca.com.
2. Fare clic su Supporto per prodotto o soluzione.
3. Selezionare CA Identity Manager nella sezione Prodotti della pagina Selezionare un prodotto o Selezionare una soluzione.

   Viene visualizzata la pagina CA Identity Manager.
4. Passare alla sezione Letture consigliate.
5. Fare clic sull'indice Documentazione informativa di CA Identity Manager.

Le matrici di supporto per la piattaforma verranno visualizzate in una pagina assieme alle versioni supportate di Identity Manager.

Installazione richiesta delle patch Solaris

Prima di installare i servizi di fornitura in Solaris 9 o 10, eseguire il download e l'installazione delle seguenti patch:

Per eseguire il download delle patch Sun Studio 10 per SDK

1. Passare al seguente URL:
   http://developers.sun.com/prodtech/cc/downloads/patches/ss10_patches.html
2. Eseguire il download e installare la patch 117830.

   Nota: Sun Studio 11 non richiede l'installazione di patch.

Per eseguire il download delle patch Solaris 9 per tutti i componenti

1. Passare al seguente URL:

   http://search.sun.com/search/onesearch/index.jsp
2. Eseguire il download e installare 9_recommended.zip

Variabile d'ambiente necessaria per l'integrazione di SiteMinder

Se durante l'installazione di Identity Manager in un sistema Solaris si attiva l'integrazione con SiteMinder, è possibile che venga visualizzato il seguente errore nel registro del server applicazioni e che Identity Manager non venga avviato:

errore "java: irreversibile: libetpki2.so: apertura non riuscita: non esistono file o directory di questo tipo"

Questo errore si verifica se l'installazione di ETPKI, che installa una libreria di crittografia necessaria per SiteMinder, non aggiunge correttamente la variabile d'ambiente CALIB.

Nota: ETPKI viene installato automaticamente dal programma di installazione di Identity Manager.

Rimedio provvisorio

Aggiungere la variabile d'ambiente CALIB nel seguente modo prima di avviare il server Identity Manager:

```
bash# export CALIB=/opt/CA/SharedComponents/ETPKI/lib
```

Installazione di ambienti Identity Manager localizzati

Sono disponibili versioni localizzate della console utente e della Guida in linea della console utente di Identity Manager. La maggior parte dei file necessari per utilizzare una versione localizzata viene installata nella seguente posizione:

dir_strumenti_amministrazione_im\samples\Localization*lingua*

dir_strumenti_amministrazione_im

Specifica il percorso di installazione degli Strumenti di amministrazione di Identity Manager.

lingua

Specifica la lingua che si desidera utilizzare.

Nota: per le istruzioni di installazione, consultare la *Guida per l'amministratore*.

Sono tuttavia disponibili file aggiuntivi obbligatori per poter utilizzare una versione localizzata di Identity Manager:

- Note di rilascio
- File della Guida in linea

  Nota: non utilizzare la versione dei file della Guida in linea disponibili nella directory *dir_strumenti_amministrazione_im*\samples\Localization*lingua.*

Questi file sono disponibili nell'area di download delle risorse di localizzazione di CA Identity Manager r12 nel sito del supporto tecnico di CA.

Per installare i file della Guida in linea

1. Eseguire il download del file ZIP delle risorse di localizzazione di CA Identity Manager r12.
2. Decomprimere i file in un sistema accessibile dal server applicazioni in cui si trova Identity Manager.
3. Copiare il file im_help_*lingua*.ZIP relativo alla lingua desiderata nella directory *IdentityMinder.ear*\user_console.war\

   IdentityMinder.ear

   Posizione di distribuzione dell'applicazione Identity Manager (IdentityManager.ear) nel server applicazioni.

   Nota: creare una copia di backup della Guida in linea predefinita prima di sostituirla con una versione localizzata. La Guida in linea predefinita verrà infatti sovrascritta dalla versione localizzata.

4. Decomprimere il file im_help.zip nella directory user_console.war.
5. Riavviare l'ambiente Identity Manager.

   La versione localizzata della Guida in linea sarà ora disponibile per l'utilizzo.

I caratteri non ASCII causano il blocco dell'installazione su sistemi di lingua diversa dall'Inglese

Durante l'installazione di Identity Manager, il programma di installazione estrae i file in una directory Temp. Su alcuni sistemi localizzati, il percorso predefinito della directory Temp contiene caratteri non ascii. Ad esempio, il percorso della directory Temp su un sistema Windows in Spagnolo è il seguente:

C:\Documents and Settings\Administrador\Configuración local\Temp

A causa dei caratteri non ASCII il programma di installazione visualizza una pagina riepilogativa di preinstallazione vuota e l'installazione non riesce.

Per evitare che l'installazione abbia un esito negativo, procedere come segue:

Modificare la variabile di ambiente tmp in modo che faccia riferimento a una cartella contenente solo caratteri ASCII.

Modifiche alla configurazione necessarie per SiteMinder in modalità Solo FIPS 140-2

Se SiteMinder viene eseguito in modalità Solo FIPS 140-2 Only, è necessario eseguire un'ulteriore operazione di configurazione.

Per configurare Identity Manager affinché funzioni con SiteMinder in modalità Solo FIPS 140-2 in WebLogic o JBoss

1. Aprire *IdentityMinder.ear*\policyserver.rar\META-INF\ra.xml.
2. Cercare il seguente elemento:

```
<config-property>
<config-property-name>FIPSMode</config-property-name>
<config-property-type>java.lang.String</config-property-type>
<config-property-value>false</config-property-value>
</config-property>
```

3. Per l'elemento <config-property-value> modificare l'impostazione da false a true.
4. Riavviare il server applicazioni.

Per configurare Identity Manager affinché funzioni con SiteMinder in modalità Solo FIPS 140-2 in WebSphere

1. Aprire la console di amministrazione di WebSphere.
2. Passare alla seguente posizione:

   Applicazioni Enterprise > IdentityMinder > Gestione moduli > policyserver.rar > IdentityMinder.PolicyServerRA > Connection factory J2C > PolicyServerConnection > Proprietà personalizzate
3. Fare clic sul valore della proprietà FIPSMode, quindi impostarne il valore su true. Fare clic su OK, quindi sul collegamento "Salva" nella parte superiore della pagina.

JBoss: configurazione supporto IPv6

Se si installa la versione JBoss di Identity Manager su un sistema che supporta IPv6, è necessario eseguire alcune procedure di configurazione.

Per configurare IPv6 su un server applicazioni JBoss, procedere come segue:

1. Aprire il file run_idm.sh, che si trova nel percorso indicato di seguito:

   jboss_installation\bin
2. Modificare *una* delle seguenti proprietà nella voce JAVA_OPTS:
   - Rimuovere il commento dalla voce seguente (solo per ambienti IPv6):

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv6Addresses=true
   - Rimuovere il commento dalla voce seguente (per ambientiIPv6/IPv4):

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv4Stack=true
3. Salvare il file.

Supporto SPML per FIPS 140-2

Per Identity Manager r12, il server SPML è conforme alla certificazione FIPS 140-2. Si consiglia di distribuire il servizio SPML su:

- Apache Tomcat Server 4.1.36 o versione successiva alla 4.1
- JDK 1.5.11 o versione successiva di JDK 1.5. Si noti che Tomcat deve essere attivato per consentire l'esecuzione in modalità SSL. Per ulteriori informazioni, consultare la sezione "Procedure di configurazione SSL" nella Guida per l'amministratore di Apache per Tomcat 4 (http://jakarta.apache.org/tomcat/).

In caso di utilizzo di CA Tomcat anziché Apache Tomcat, Identity Manager r12 richiede l'implementazione di due rimedi provvisori per SPML:

- In caso di utilizzo di JDK 1.4.xx con CA Tomcat, la certificazione FIPS 140-2 deve essere disattivata. JDK 1.4.xx non è compatibile con CA Tomcat perché la libreria RSA Jsafe CryptoJ 4.0 necessaria per il supporto della certificazione FIPS 140-2 non può essere impostata come primo provider di protezione in JDK1.4.

  Per disattivare il supporto della certificazione FIPS 140-2, impostare il flag JVM "-Dcom.ca.commons.security.fips=false" durante l'avvio di Tomcat.

  - In caso di esecuzione di Tomcat dalla riga di comando, è possibile includere il flag JVM catalina.bat. Ulteriori dettagli sono disponibili nel file batch stesso.
  - In caso di esecuzione di Tomcat come servizio di Windows, impostare il flag nel seguente modo:

    a. Utilizzando l'Editor del Registro di sistema passare alla chiave "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CA Tomcat 4.1.29 eTrustIAMWebServer\Parameters"

    b. Aggiungere un valore stringa denominato "JVM Option Number n" dove "n" rappresenta il numero successivo rispetto al parametro JVM precedente. Per il valore specificare:

    Dcom.ca.commons.security.fips=false

    c. Aumentare di un'unità il valore "JVM Option Count" di Modifica valore DWORD per il parametro appena aggiunto.

- In caso di utilizzo di JDK 1.5 con CA Tomcat, si verificherà un problema di incompatibilità. Per risolvere il problema, procedere come segue:

  a. Rimuovere manualmente le due librerie Xerces (xercesImpl.jar e xmlParserAPIs.jar) da %TOMCATHOME%\common\endorsed.

  b. Riavviare Tomcat.

Modifiche all'architettura dei connettori z/OS

I connettori z/OS (CA ACF2, CA Top Secret e RACF) sono stati riarchitettati a scopi prestazionali, al fine di utilizzare CA LDAP Server per z/OS anziché CA DSI Server su z/OS.

Prima di configurare un qualsiasi connettore z/OS, è necessario installare CA LDAP Server per z/OS r12, il quale può essere scaricato sul sito Web support.ca.com.

Posizione di eTrust Directory

Lo schema relativo alla directory di fornitura è installato su eTrust Directory. È possibile installare eTrust Directory dal supporto di installazione di Identity Manager.

È richiesta la correzione del problema prima di disinstallare eTrust Directory

Se è necessario disinstallare eTrust Directory da un sistema Windows, applicare la patch prima di avviare la procedura di disinstallazione.

Se la patch non viene applicata, la procedura di disinstallazione potrebbe rimuovere i file della licenza necessari al funzionamento di altri prodotti CA.

È possibile scaricare la patch sul sito del supporto tecnico di CA.

Per trovare la patch:

1. Accedere a support.ca.com.

   Viene visualizzato il sito del supporto tecnico di CA.

2. Fare clic su Licensing nell'elenco di collegamenti, sul lato a sinistra della pagina.

3. Fare clic su License Package 1.8 is Now Available.

   Si apre una pagina in cui sono descritte le modifiche relative al pacchetto della licenza e in cui è presente un collegamento per scaricarlo.

4. Seguire le istruzioni per il download e installare la patch per Windows.

Capitolo 6: Problemi noti

Questa sezione contiene i seguenti argomenti:

Generale

Di seguito sono elencati i problemi noti generali di Identity Manager r12.

Il file EAR di Identity Manager non viene distribuito automaticamente con WebLogic

Se si utilizza WebLogic 8 o 9 in modalità di produzione, il file EAR di Identity Manager non viene distribuito automaticamente la prima volta che si avvia il server applicazioni o dopo un'installazione o aggiornamento. In tal caso, distribuire IdentityMinder.ear manualmente dalla cartella user_projects\applications.

Flussi di lavoro e Membri gruppo come approvatori

Se il processo di un flusso di lavoro viene configurato in Workpoint Designer affinché disponga di membri gruppo specifici come relativi approvatori, la creazione di un elemento del flusso di lavoro potrebbe non essere attuabile in un evento sotto il controllo del flusso di lavoro e la sessione attività potrebbe avere esito negativo.

Per risolvere il problema, impostare il controllo delle attività da parte del flusso di lavoro utilizzando il metodo basato su modelli (con i modelli SingleStepApproval o TwoStageApprovalProcess), quindi definire i membri gruppo in modo da farli risultare approvatori (o resolver partecipanti).

L'impostazione delle proprietà del nuovo Workpoint potrebbe non essere necessaria

Identity Manager include una nuova versione di Workpoint. In questa versione, è possibile configurare più proprietà in GeneralMonitor.properties e workpoint-server.properties. Queste nuove proprietà sono opzionali e devono essere aggiunte solo se necessario.

Le nuove proprietà del flusso di lavoro sono le seguenti:

- Nel file GeneralMonitor.properties:
  - #JMX_HTML_ADAPTOR_PORT=9092

    Per impostazione predefinita, questa proprietà sono convertite in commenti. La proprietà quando è impostata su true, abilita una pagina HTML che utilizza una scheda Sun JMX generica, ossia una porta Web non protetta, separata dall'applicazione della Console di gestione Workpoint. Si consiglia di lasciare tali proprietà convertite in commenti o di impostarle su false e utilizzare la Console di gestione Workpoint per consentire a JMX di accedere a Workpoint.
  - JOB_ERROR_STATE_ON_MAIL_ERROR=false

    Questa proprietà è applicabile solo per gli utenti che utilizzando la funzione e-mail di Workpoint. Questa proprietà controlla la gestione degli errori nel mail monitor. Se gli utenti di Identity Manager utilizzano la funzione e-mail di Workpoint, questa proprietà è applicabile.

    Nota: JOB_ERROR_STATE_ON_MAIL_ERROR è configurata su true per impostazione predefinita, se non diversamente specificata. È possibile impostarla su false se si utilizza la funzione e-mail di Workflow, ma gli errori relativi alla posta elettronica interferirebbero con lo stato del processo.
  - ENABLE_SCRIPT_TASK_GROUPING=false

    Questa proprietà controlla che lo script monitor raggruppi tutti gli script concomitanti eseguiti dallo stesso processo. Se impostata su true, tutti gli script di un particolare processo vengono assegnati allo stesso thread utente, in cui verranno eseguiti singolarmente. Ciò risulta utile per evitare eccezioni di simultaneità quando più attività in un processo utilizzano uno script asincrono per l'automazione e possono risultare attive allo stesso tempo.

    Se gli script del flusso di lavoro sono personalizzati e si verificano eccezioni di simultaneità, si consiglia di esaminare questa proprietà.

    Altre proprietà e-mail e proprietà correlate sono incluse nel file GeneralMonitor.properties.

- Nel file workpoint-server.properties:
  - server.automated.delay=500

    Questa proprietà controlla i nodi server automatizzati, per garantire che tali nodi non siano serviti sulla coda prima che la transazione del database che li ha posti in coda renda tale condizione permanente. Ciò impedirà eventuali errori dei nodi server automatizzati, a causa dei problemi di tempo. Questa proprietà è consigliata quando sono in uso i nodi server automatizzati.

Impossibile creare una copia di un gestore di attributi logici

Quando si cerca di creare una copia di un gestore di attributi logici nella console utente, verrà visualizzato il seguente errore:

"Questo oggetto non è collegato"

La creazione di un nuovo gestore di attributi logici, non basato su un gestore di attributi logici esistente, funziona correttamente.

Utilizzo dei filtri di gruppo nei Criteri di ruolo

Quando Identity Manager gestisce un archivio utente in un database relazionale, i filtri di gruppo nei criteri di amministrazione e membro potrebbero non funzionare correttamente. Ad esempio, se viene specificato un filtro quale "Utenti che sono membri di un gruppo il cui nome inizia con la lettera A" in un criterio membri, Identity Manager potrebbe applicare erroneamente il criterio a tutti gli utenti, anziché applicarlo solo a quelli il cui gruppo inizia con la lettera A.

Per evitare che ciò accada, assicurarsi che le tabelle, tblGroupMembers e tblGroupAdministrators siano correttamente definite per l'oggetto utente nel file di configurazione della directory (directory.xml).

La definizione dell'oggetto utente nella directory directory.xml deve essere analoga a quella riportata di seguito:

```
<ImsManagedObject name="User" description="My Users" objecttype="USER">
<!-- COMMENT Table -->
    <Table name="tblUsers" primary="true" />
    <Table name="tblUserAddress">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserRoles">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserDelegators">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserPasswordhints">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserIdentityPolicy">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblOrganizations">
    <Reference childcol="id" primarycol="org"/>
    </Table>

    <Table name="tblGroupMemebers">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblGroupAdmins">
    <Reference childcol="userid" primarycol="id"/>
    </Table>
```

Dopo aver modificato il file di configurazione della directory, importarlo utilizzando la Console di gestione.

Nota: per ulteriori informazioni sulla modifica dei file di configurazione della directory, fare riferimento alla *Guida alla configurazione*.

Configurazione degli schermi di ricerca attività e ruoli

Quando si configurano gli schermi di ricerca per attività o ruoli, è possibili limitare il numero dei risultati restituiti dalla ricerca, impostando l'opzione "Mostra solo oggetti che rispettano le regole seguenti". Gli attributi utilizzati durante la configurazione di questa opzione, non devono essere indicati come campi di ricerca disponibili negli schermi di ricerca.

Ad esempio, quando si configura lo schermo di ricerca in modo che visualizzi solo i ruoli dove l'attributo Abilitato è impostato su sì, è necessario rimuovere il suddetto attributo dall'elenco di attributi che l'utente può specificare nei criteri di ricerca.

In caso contrario, i criteri specificati dall'utente verranno ignorati.

Creazione dell'ambiente Identity Manager nei browser Firefox

Se si accede alla console di gestione mediante un browser Firefox, la creazione dell'ambiente Identity Manager può risultare lenta e potrebbe sembrare che si blocchi. In questi casi, la creazione dell'ambiente continua, ma il browser non viene aggiornato. Il completamento della creazione non viene pertanto visualizzato.

Nota: se si chiude la finestra del browser, Identity Manager continua a creare l'ambiente.

Aggiornamenti

Le seguenti problematiche fanno riferimento agli aggiornamenti di Identity Manager r12.

Gli endpoint MS SQL e Oracle non sono disponibili dopo l'aggiornamento da eTrust Admin 8.1 SP2

Dopo aver eseguito l'aggiornamento da eTrust Admin 8.1 SP2 a Identity Manager r12, gli endpoint MS SQL e Oracle acquisiti prima dell'aggiornamento devono essere riconfigurati manualmente tramite Gestione fornitura, al fine di utilizzare gli URL JDBC anziché i nomi di origine dati (DSN). Ciò è dovuto al passaggio da SuperAgent al server di connessione Java per la gestione degli endpoint MS SQL e Oracle.

Oracle: modificare i dettagli nel foglio delle proprietà dell'endpoint Oracle.

Esempio:

```
jdbc:oracle:thin:@oracle_server_host:1521:ORACLE
```

MS SQL: fare clic con il pulsante destro del mouse sull'endpoint, quindi su Personalizzato selezionare Modifica password Admin. A questo punto è possibile modificare le credenziali di connessione e dell'URL, senza visualizzare i dettagli degli altri endpoint.

Esempio:

```
jdbc:sqlserver://serverHost:1433;instanceName=instance1
```

Nota: è possibile trovare le procedure di migrazione e un elenco di sintassi di URL possibili nel capitolo 4: Connettori del database della *Guida ai connettori*.

L'agente remoto UNIX non è disponibile per la piattaforma Solaris x86 (Intel)

Nel pacchetto dell'agente remoto Unix mancano file necessari per l'esecuzione dell'installazione o dell'aggiornamento dell'agente remoto UNIX nella piattaforma Solaris x86 (Intel).

Modifiche all'architettura dei connettori z/OS

I connettori z/OS (CA ACF2, CA Top Secret e RACF) sono stati riarchitettati a scopi prestazionali, al fine di utilizzare CA LDAP Server per z/OS anziché CA DSI Server su z/OS.

Prima di configurare un qualsiasi connettore z/OS, è necessario installare CA LDAP Server per z/OS r12, il quale può essere scaricato sul sito Web support.ca.com.

Dopo aver eseguito l'aggiornamento a Identity Manager r12, applicare le procedure descritte di seguito per ciascun endpoint definito sul sistema:

Dal visualizzatore delle attività dell'endpoint

1. Selezionare l'endpoint RACF, CA ACF2, CA o Top Secret dal tipo di oggetto
2. Fare clic sul pulsante Cerca. Con il pulsante destro del mouse fare clic sull'endpoint e selezionarne le proprietà. Immettere le seguenti informazioni:

   Nella sezione Informazioni server mainframe:

   - **Indirizzo IP/Nome computer** specifica l'indirizzo IP del sistema RACF gestito, su cui è configurato ed è in esecuzione CA LDAP Server.
   - **Porta LDAP** specifica il numero della porta indicato durante l'installazione di CA LDAP Server per z/OS. Se non si conosce il numero di porta LDAP mainframe, fare riferimento alla sezione "Controllo delle informazioni di configurazione di CA LDAP Server per z/OS".
   - **Suffisso LDAP** specifica il suffisso da utilizzare per questo endpoint. Questa casella combinata viene compilata automaticamente con tutti i suffissi disponibili e validi, quando si seleziona il pulsante "Ottieni suffissi". È possibile recuperare i suffissi dopo aver specificato valori validi nei campi relativi a Porta LDAP mainframe, Indirizzo IP mainframe e Nome computer

Rapporti

Le seguenti problematiche fanno riferimento alla generazione di rapporti di Identity Manager r12.

Limitazione della generazione di rapporti

Più snapshot associati a un'unica attività di generazione di rapporti non devono utilizzare la stessa ora di ricorrenza.

Funzionamento non corretto del parametro satisfy=All nel file XML

In un file XML dei parametri snapshot i parametri satisfy=all e satisfy=any hanno lo stesso funzionamento del parametro satisfy=any (simile a un operatore OR).

Attivazione di cookie per l'attività Visualizzazione rapporti personali

Per visualizzare i rapporti in Identity Manager utilizzando l'attività Visualizzazione rapporti personali, attivare i cookie delle sessioni di terze parti nel browser.

ExportALL.xml e Environments senza supporto organizzazione

Quando si utilizza un file XML dei parametri snapshot (ad esempio: ExportAll.xml) che esporta gli attributi e gli oggetti dell'organizzazione, si verifica un'eccezione quando l'ambiente non dispone di supporto per le organizzazioni. Per risolvere il problema, convertire in commento l'oggetto organizzazione e l'attributo nel file ExportAll.xml file.

Fornitura

Le abbreviazioni relative ai componenti di fornitura per il seguente elenco di problemi ed errori, sono indicate di seguito:

- ACC: connettore controllo accessi di CA
- ADS: connettore servizi di Active Directory
- DBZ: connettore database universale DB2 per z/OS
- DYN: connettore dinamico
- E2K: connettore Exchange 2000
- EEM: connettore Embedded Entitlements Manager
- ETC: UNIX ETC
- FND: connettore applicazioni Oracle
- INS: installazione
- KRB: connettore Kerberos
- LND: connettore Lotus Notes/Domino
- NDS: connettore Novell Directory Services
- N16: agente remoto Windows NT
- AS4: connettore OS/400
- PKI: connettore Entrust PKI
- PLS: CA SSO per connettore server dei criteri avanzati
- PSA: agente di sincronizzazione password
- RSA: connettore RSA SecurID
- SAP: connettore SAP
- SBL: connettore Siebel
- UPO: connettore di fornitura universale
- VMS: connettore OpenVMS
- z/OS: connettori CA ACF2, CA Top Secret, RACF

Generale

Di seguito sono elencati i problemi generali relativi alla fornitura in Identity Manager r12.

Sincronizzazione degli account per l'attività Reimposta password utente

Per attivare la fornitura per un ambiente Identity Manager, importare un file di configurazione denominato ProvisioningOnly-RoleDefinitions.xml, che crea i ruoli e le attività per la fornitura di utenti.

In tale file, per impostazione predefinita la sincronizzazione degli account per l'attività Reimposta password utente è impostata su Disattivata. Prima di attivare la fornitura, la sincronizzazione è impostata su Al completamento dell'attività.

Per utilizzare l'attività Reimposta password utente per attivare la sincronizzazione degli account, impostare l'opzione Sincronizzazione account dopo l'importazione del file ProvisioningOnly-RoleDefinitions.xml per abilitare la fornitura.

La console utente non riesce a esplorare e correlare alcuni tipi di endpoint

Le attività di esplorazione e correlazione nella console utente non riescono a trovare i seguenti tipi di endpoint:

- Kerberos
- UNIX NIS
- Entrust PKI
- Siebel
- Database universale per z/OS
- Tipi di endpoint sviluppati personalizzati

Per esplorare e correlare tali tipi di endpoint, è possibile utilizzare Gestione fornitura. Quindi è possibile eseguire funzioni account di routine nella console utente, quali l'assegnazione di un account su tali endpoint.

Esplorazione e correlazione dei lavori in un fuso orario

Nella console utente è possibile pianificare la definizione Esplora e correla. Questa operazione richiede che il browser client e il server condividano lo stesso fuso orario. Ad esempio, se l'ora del client è 22.00 di martedì mentre l'ora del server è 07.00, la definizione Esplora e correla non funzionerà correttamente.

Core dump del server di fornitura su Solaris

Il server di fornitura su Solaris genera un file core all'arresto del servizio.

Ciò non influisce in alcun modo sulle funzionalità e può essere tranquillamente ignorato.

Il programma di installazione della directory di fornitura richiede un nome host risolto correttamente

Il programma di istallazione richiede un nome host con una risoluzione nomi configurata correttamente, quando si installano la directory di fornitura e il server di fornitura sullo stesso computer. L'installazione del server di fornitura non riuscirà o genererà risultati non previsti, se il computer non risolve il relativo nome computer nell'indirizzo IP desiderato. Gli scenari possibili sono due.

- Viene generato un risultato di risoluzione nome differente per FQDN e il nome host (ad esempio, in una rete IPv4/6, si registra un indirizzo IPv6 nel DNS, ma si dispone di un indirizzo IPv4 per il nome host tramite net bios o il file host). Se si configura la directory di fornitura affinché ascolti solo IPV6, quindi si installa il server di fornitura affinché utilizzi FQDN, l'installazione non riuscirà perché il programma di installazione sta tentando di risolvere il nome host e non l'FQDN in alcune fasi dell'installazione. Per risolvere il problema, aggiungere il nome host e il relativo indirizzo IPv6 al file host. Tuttavia, questa non rappresenta la configurazione corretta.
- Su una macchina che non dispone di DNS o altri risultati di nomi, se si tenta l'installazione della directory di fornitura e del server di fornitura utilizzando un indirizzo IP, l'installazione non riuscirà.

  Note: CA non supporta l'installazione mediante indirizzo IP.

Alcune configurazioni di dominio eseguite con modifiche simultanee della password utente globale provocano l'arresto del server di fornitura

Se la configurazione del dominio "Server Identity Manager/Usa criteri password esterni" è impostata su sì e si eseguono più modifiche della password utente globale. Da ciò ne deriva una riduzione delle prestazioni e l'eventuale arresto del server di fornitura.

L'accesso a Solaris ECS al di sopra del livello INFO può influire negativamente sulle prestazioni del server di fornitura

L'abilitazione dell'accesso a ECS al di sopra del livello INFO causa la scrittura dei registri prima di ricevere una risposta. Pertanto, la richiesta subisce un ritardo e il registro viene scritto. Se le prestazioni del server di fornitura non sono soddisfacenti quando si utilizza l'accesso a ECS, per risolvere il problema si consiglia di disattivare il servizio.

Gli aggiornamenti di SPML non riescono quando JIAM specifica nomi di classe oggetto non validi

Talvolta l'interfaccia API JIAM inizia a utilizzare nomi di classe oggetto ridotti nelle richieste inviate al server di fornitura, il quale rifiuta la richiesta e genera un errore che indica che si è verificato un errore di coerenza interno. Ad esempio, quando si esegue l'aggiornamento dell'oggetto "eTSBLDirectory", al server di fornitura viene inviata la classe oggetto "eTDirectory" errata. Per risolvere il problema, riavviare il servizio SPML.

Caratteri speciali nei nomi utenti globali

La funzionalità Gestione fornitura consente di creare nomi utenti globali contenenti caratteri speciali quali, ad esempio, la barra rovesciata (\). Tuttavia, il server Identity Manager non supporta i nomi utente contenenti caratteri speciali.

Quando in Gestione fornitura viene creato un utente globale contenente un carattere speciale, Identity Manager cerca di creare un utente corrispondente nell'archivio utenti di Identity Manager. Si verificano alcuni errori e l'attività Crea utente ha esito negativo nell'archivio utenti di Identity Manager.

Si verificano errori anche se si cerca di eliminare un utente globale contenente caratteri speciali in Gestione fornitura.

Gestione fornitura contiene riferimenti SAWI/DAWI obsoleti

In Gestione fornitura sono disponibili finestre di dialogo contenenti controlli non più supportati per le funzionalità SAWI e DAWI. Utilizzare le funzionalità self-service di Identity Manager anziché SAWI o DAWI.

Durante l'aggiunta di un endpoint viene visualizzato un messaggio di errore che indica che l'endpoint esiste già

Se si elimina e si aggiunge nuovamente un endpoint con lo stesso nome, talvolta il server di fornitura genera un errore, segnalando che l'endpoint esiste già. Ciò avviene quando si configurano più server di connessione che gestiscono quel dato endpoint. L'errore è dovuto a un problema che si verifica durante l'eliminazione dell'endpoint, durante la quale non tutti i server di connessione vengono notificati dell'eliminazione dell'endpoint.

Per risolvere il problema, riavviare tutti i server di connessione configurati per la gestione dell'endpoint.

Server di connessione Java (CS)

I problemi indicati di seguito sono relativi al server di connessione Java in Identity Manager r12.

L'esplorazione del connettore Java non riesce quando si utilizza la sequenza caratteri " / per rappresentare nomi distinti

La gestione della seguente sequenza a due caratteri da parte del server di connessione Java è un problema irrisolto:

"/

Ciò è fondamentale nella gestione dei nomi composti utilizzati dall' interfaccia API JNDI, al fine di rappresentare i nomi distinti utilizzati in molteplici piattaforme tecnologiche.

Per ulteriori informazioni sui caratteri speciali nei nomi distinti passati al server di connessione Java, fare riferimento a LDAP RFC 2253 all'indirizzo:

http://ietf.org

e a JavaDoc per javax.naming.ldap.LdapName

Errore di puntatore NULL in Connector Xpress

Se si cerca di modificare le informazioni di routing del server di connessione facendo clic con il pulsante destro del mouse su un tipo di endpoint e quindi scegliendo di impostare la gestione CS oppure direttamente modificando le configurazioni CS negli ambienti con più server di fornitura utilizzando Connector Xpress, è possibile che in Connector Xpress venga visualizzato un errore di puntatore NULL. Se è necessario eseguire il routing avanzato del server di connessione, utilizzare lo strumento csfconfig.

Riavvio del servizio CS Java non riuscito mediante i servizi di Windows

Durante il riavvio del servizio CS Java utilizzando i servizi di Windows, è possibile avviare il servizio CS Java prima del suo completo arresto. Ciò impedisce l'avvio del servizio. Se si verifica questo problema, utilizzare i pulsanti di arresto e riavvio anziché i pulsanti di riavvio disponibili nel Pannello di controllo del servizio di Windows.

Messaggio di errore errato se non si seleziona una stored procedure

Se non si seleziona una stored procedure nell'elenco a discesa Seleziona una procedura negli schermi Mappa tabella nella procedura guidata di Connector Xpress e si fa clic su Avanti, viene visualizzato il seguente messaggio di errore errato:

Specificare una tabella da mappare.

Il messaggio corretto è:

Specificare una procedura da mappare.

I contenitori esplorati dell'endpoint DYN JNDI non sono presenti in Gestione fornitura

Dopo aver eseguito un'esplorazione di livello singolo di un contenitore su endpoint DYN JNDI appena acquisiti, il pannello relativo al contenuto di Gestione fornitura non visualizza il contenitore appena esplorato, anche se il conteggio di esplorazione indica l'aggiunta del nuovo record. Per forzare la visualizzazione del contenitore, chiudere e riaprire Gestione fornitura.

Gli attributi sospesi del modello dell'account DYN sono visualizzati in grassetto in Gestione fornitura

Gestione fornitura visualizza in grassetto l'attributo di stato dell'account per i modelli account DYN, il quale indica erroneamente che il suddetto è un attributo di capacità.

Le etichette degli attributi di capacità DYN possono risultare troncate in Gestione fornitura

Gli attributi di capacità specificati durante la creazione dei tipi di endpoint DYN JDBC o DYN JNDI in Connector Xpress potrebbero presentare etichette troncate o mancanti quando visualizzati su Gestione fornitura. Per risolvere il problema, specificare un carattere aggiuntivo alla fine dell'etichetta, ad esempio "*Nome etichetta a*", quando si immette displayName in Connector Xpress. Ciò non avviene se si utilizzano gli attributi di capacità appartenenza.

È possibile modificare anche i metadati esistenti, attenendosi a una delle procedure descritte di seguito:

Dopo aver caricato il progetto salvato in Connector Xpress

- Eseguire la procedura guidata
- Espandere la struttura dei metadati, accedere a Classi -> eTDYNPolicy -> Proprietà -> Attributo di capacità -> Metadati e modificare il valore displayName.

Se si sceglie uno dei metodi appena descritti per modificare i metadati esistenti per il tipo di endpoint DYN, assicurarsi di aggiornare il suddetto con i nuovi metadati.

Connettori

Le seguenti problematiche fanno riferimento ai connettori di fornitura di Identity Manager r12.

Risultati errati restituiti dalla ricerca di una sottostruttura con connettore ADS

Durante una ricerca di una sottostruttura a fronte di una sottostruttura contenente Unità organizzative con un elevato numero di oggetti in ciascuna di queste unità, la ricerca, erroneamente, non restituisce alcun oggetto. Ad esempio, con un limite di dimensioni ricerca impostato su 500 e il numero di oggetti in ciascuna OU superiore al suddetto limite, non viene restituito alcun risultato. Anche se il filtro della ricerca viene ristretto a un valore inferiore a 500, la ricerca potrebbe non restituire alcun oggetto. Per risolvere il problema, aumentare il limite di dimensioni della ricerca.

Evitare di inserire date di scadenza ADS successive all'anno 2038

L'impostazione di una data di scadenza per un account ADS su una data successiva all'anno 2038, causa l'arresto di Gestione fornitura.

IE7 non supporta il connettore EEM

Il connettore EEM non è supportato se il server di connessione C++ (CCS) per lo specifico connettore EEM è installato su una macchina con IE7.

Nota: nella documentazione del prodotto relativa a Identity Manager r12, per EEM (Embedded Entitlements Manager) si intende un connettore EIAM (Embedded Identity and Access Manager)

Visualizzazione dei modelli di account EEM con Gestione fornitura

Gestione fornitura potrebbe non rispondere durante la visualizzazione dei modelli di account EEM.

Per risolvere il problema, spegnere e riavviare Gestione fornitura.

Riaprire Gestione fornitura per acquisire un nuovo endpoint EEM

Dopo aver impostato un nome host durante un'acquisizione, è necessario chiudere e riaprire Gestione fornitura per acquisire un altro endpoint. Questo è valido anche in caso di annullamento dell'operazione.

Impossibile selezionare o modificare gli attributi su un modello di account EEM

Quando si creano modelli di account per un endpoint EEM, è necessario selezionare la scheda Proprietà applicazione dopo aver selezionato l'endpoint, quindi fare clic su OK per terminare il processo di creazione del modello di account.

L'acquisizione dell'endpoint DB2 z/OS causa l'arresto del server CCS

I connettori DB2 UDB e DB2 z/OS non devono instradare le richieste sullo stesso server di connessione C++ (CCS).

Per risolvere il problema, installare un secondo server CCS su un altro computer, in modo da ospitare ciascun connettore DB2 UDB e DB2 z/OS sul proprio server di connessione C++.

Aggiornamento automatico dell'agente remoto ETC UNIX non supportato

Gli aggiornamenti automatici di un agente remoto ETC UNIX da eTrust Admin r8.1 SP2 a Identity Manager r12 non sono supportati. L'aggiornamento deve essere eseguito con l'intervento dell'utente.

L'agente remoto ETC su sistema operativo Linux in esecuzione su S390 genera un errore

Il tentativo di installazione dell'agente remoto ETC su un sistema operativo Linux in esecuzione su un host S390, genera il seguente errore, il quale indica che si è verificato un errore durante il caricamento delle librerie condivise e che non è possibile aprire il file oggetto condiviso, poiché non esiste tale file o directory:

"linux098:/home/marty/LinuxS390 # ./IdentityManager.LinuxS390.sh
lsm.exe: error while loading shared libraries: libncurses.so.4: cannot open shared object file: No such file or directory."

Per risolvere il problema, è necessario individuare la versione 4 di ncurses del sistema operativo e installarla.

L'esecuzione del comando Cafthost genera un errore per HP-UX UNIX

È possibile che si verifichi l'errore "Errore bus (core dump)" quando si esegue il comando descritto di seguito:

```
cafthost -a <nome_host>
```

Per aggiungere host, modificare manualmente il file di configurazione "cafthost.cfg" utilizzando un editor di file di testo nella directory "`cat /etc/catngcampath`", quindi aggiungere ciascun host su una nuova riga.

La disinstallazione dell'agente remoto ETC genera file orfani

Quando l'agente remoto ETC viene aggiornato da r8.1SP2 a r12, è possibile che alcuni file rimangano orfani. Se tali file non vengono utilizzati da altri pacchetti di installazione, è possibile rimuoverli:

- /usr/bin/uxsautil
- `cat /etc/catngdmopath.tng`/bin/uxsautil
- `cat /etc/catngdmopath.tng`/scripts/Config
- `cat /etc/catngdmopath.tng`/etc/ExitSetup.ini
- `cat /etc/catngdmopath.tng`/scripts/caftexec
- `cat /etc/catngdmopath.tng`/scripts/caftexec.cfg
- `cat /etc/catngdmopath.tng`/setup.gif

La modifica di VMS che consente di eliminare i diritti account non riesce con SPML

Non è possibile eliminare un valore dall'attributo accountRights sull'account VMS utilizzando SPML. Il client SPML restituisce un messaggio che indica l'esito positivo dell'operazione, ma l'account non è stato aggiornato.

Per risolvere il problema, utilizzare Gestione fornitura per eseguire tali modifiche.

Impossibile impostare una password secondaria per gli account OpenVMS

L'utilità dell'agente remoto OpenVMS 'vmsautil' non applica la semantica della password PRIMARIA/SECONDARIA OpenVMS per gli account utente. Se si tenta di specificare una password secondaria ma non è stata impostata alcuna password primaria, l'operazione non riesce e viene visualizzato un messaggio di errore che indica che la password è troppo breve.

Per risolvere il problema, reimpostare sempre la password primaria quando si tenta di impostare la password secondaria dell'account.

Istruzione mancante in CAM/CAFT per OpenVMS

Nel file ETRUST_ADMIN_OPENVMS_INSTALLATION.TXT mancano informazioni su come configurare CAMCAFT.EXE in un sistema OpenVMS. Il nome simbolico CAFTHOST deve essere definito prima di installare CAM/CAFT. Per definire CAFTHOST, aggiungere il seguente comando al file LOGIN.COM:

```
CAFTHOST :==$CAPOLY$BIN:CAFTHOST.EXE
```

Accedere nuovamente al sistema OpenVMS.

L'attributo eTVMSPWDLifeTime di VMS non è sincronizzato

L'attributo relativo alla durata utile della password (eTVMSPWDLifeTime) non risulta sincronizzato dopo l'esecuzione dell'operazione "Controllo sincronizzazione account", se l'attributo "Nessuna scadenza" del modello di account è impostato su true (verificato).

Lo stato dell'account VMS viene indicato erroneamente da SPML come falso

Se l'account VMS viene sospeso, Gestione fornitura indica correttamente che lo stato dell'account è "Attivo (sospeso in eTrust Admin)", tuttavia SPML riporta tale informazione come falsa

Impossibile impostare i flag per la password di VMS

L'attributo eTVMSPwdFlags non è stato impostato correttamente durante l'operazione di aggiunta o modifica dell'account, se la richiesta non imposta un valore anche per eTVMSAccessFlags.

Per risolvere il problema, è necessario che la richiesta di aggiunta o modifica contenga un valore per l'attributo eTVMSAccessFlags e l'attributo eTVMSPwdFlags.

L'attributo di migrazione password di VMS non è sincronizzato

Qualsiasi account VMS o modello di account con il campo MIGRATEPW impostato su true (verificato), indica che eTVMSPwdFlags non è sincronizzato dopo l'esecuzione dell'operazione "Controllo sincronizzazione account".

Sospensione account VMS

La sospensione di un account a livello di account tramite Gestione fornitura viene eseguita correttamente, tuttavia l'account non mantiene lo stato "Sospeso" nella pagina delle proprietà e viene modificato in "Attivo" quando si applicano le modifiche. Pertanto, si dispone di un account sospeso, ma la pagina delle proprietà indica che il suddetto account è "Attivo", quindi non può essere reso nuovamente "Attivo".

Non vi è una soluzione al problema operando sull'account. L'unica soluzione consiste nel correlare l'account a un utente globale, quindi controllare la sospensione dell'account tramite la sospensione dell'utente globale

I nomi utente VMS non possono contenere caratteri Unicode non escape

Se si tenta di creare un account VMS con un nome non valido, il server di fornitura installato su Solaris potrebbe subire un arresto.

Il connettore NDS non riesce a esplorare nuovi contenitori

La prima esplorazione cerca di trovare e aggiungere i contenitori dopo l'acquisizione di un endpoint NDS. Se i contenitori vengono aggiunti utilizzando gli strumenti locali NDS e quindi si cerca di esplorare nuovamente l'endpoint, nella struttura non vengono visualizzati i contenitori appena aggiunti e le relative sottovoci.

È necessario rimuovere l'endpoint da Gestione fornitura e quindi acquisirlo nuovamente ed esplorarlo, al fine di visualizzare i nuovi contenitori.

La descrizione del connettore NDS è un campo a valore singolo

Nel connettore NDS la descrizione dell'account è un campo a valore singolo, ma nell'endpoint NDS la descrizione dell'account è un campo multivalore.

Rimuovere o modificare la variabile di ambiente dopo l'aggiornamento, per evitare eventuali problemi con il tipo di endpoint del connettore UPO

Durante l'aggiornamento remoto di un SuperAgent remoto al server di connessione C++ r12, la variabile di ambiente ETAHOME potrebbe contenere un percorso di installazione del server CSS non valido, causando in tal modo problemi con il tipo di endpoint del connettore UPO. È necessario installare manualmente la variabile di ambiente ETAHOME oppure modificarla in base al percorso di installazione corretto del server CCS, dopo l'aggiornamento e prima di provare ad acquisire o utilizzare l'endpoint UPO.

L'acquisizione dell'endpoint UPO non convalida il campo del dominio

Verrà acquisito un endpoint UPO con un valore non valido specificato nell'attributo relativo al dominio, tuttavia l'endpoint durante l'esplorazione genererà un messaggio di errore, il quale indicherà che i diritti di accesso sono insufficienti e la ricerca del server di connessione non è riuscita.

Per risolvere il problema, fare clic con il pulsante destro del mouse sull'endpoint in Gestione fornitura e selezionare Personalizzato -> Aggiorna credenziali... e specificare il valore corretto per il dominio.

Il controllo richiesto del parametro Kernel non è stato eseguito prima dell'aggiornamento di eTrust Common Services a Enterprise Common Services su Solaris

Il controllo richiesto del parametro Kernel non è stato eseguito sui prodotti che effettuano l'aggiornamento di eTrust Common Services a Enterprise Common Services su Solaris (generalmente ciò si riferisce a Solaris 9 e non a Solaris 10). A seguito di un messaggio di avvertenza è possibile continuare l'installazione anziché arrestarla, se i parametri kernel non sono sufficienti. Ciò influisce su quanto indicato di seguito:

- Agente remoto RSA su Solaris
- IMPS su Solaris
- IMPS SDK

Per risolvere il problema, procedere come segue:

Esegui

```
'<product installer dir>/solaris/ecs-installation/eCSinstall.sh'
```

Se i parametri kernel non soddisfano i requisiti, viene visualizzato un messaggio informativo. Se i requisiti del kernel vengono soddisfatti, il programma di installazione viene inizializzato

Impossibile duplicare gli account KRB

In Gestione fornitura il tentativo di duplicare un account Kerberos potrebbe generare l'errore: "eTKRBFullNameCorrelate non trovato nel registro degli attributi. (...) - Codice restituito: 111". Per risolvere questo problema, aggiungere un nuovo account anziché duplicare l'account.

Errore durante l'impostazione di un'area di autenticazione non valida durante l'acquisizione di un endpoint KRB

Se si cerca di acquisire un endpoint KRB e si specifica un valore non valido per l'area di autenticazione, verrà generato un messaggio di errore di tipo puntatore NULL.

L'endpoint di sicurezza z/OS causa l'arresto del server di fornitura su Solaris

Se l'endpoint non riesce a collegarsi a CA LDAP Server per z/OS r12, il server di fornitura si arresta.

Per risolvere il problema, assicurarsi di configurare l'endpoint immettendo informazioni di connessione valide

Sincronizzazione z/OS mediante endpoint LDS

L'agente di sincronizzazione LDS non è incluso sul DVD di Identity Manager r12. Nel caso sia richiesto il suddetto agente, contattare l'assistenza tecnica.

Viene visualizzato un messaggio di errore relativo a E2K durante la gestione dei diritti relativi alla casella postale su Exchange 2007

Non è possibile gestire i diritti delle caselle postali su Exchange 2007. Viene visualizzato il messaggio di errore che indica "Messaggio CAFT: accesso negato oppure il comando non è stato eseguito".

Viene visualizzato un messaggio di errore relativo a CAFT E2K durante la gestione dei diritti relativi alla casella postale

In fase di gestione dei diritti della casella postale viene visualizzato un messaggio di errore che indica "Messaggio CAFT: accesso negato oppure il comando non è stato eseguito". Tale messaggio può visualizzarsi anche se l'agente remoto di Exchange è configurato correttamente.

Ciò avviene quando l'elenco dei diritti della casella postale contiene più privilegi per lo stesso oggetto e generalmente si verifica quando gli oggetti Exchange gestiti ereditano i diritti dall'oggetto principale.

Non sono consentiti più indirizzi e-mail primari per E2K

È possibile utilizzare Gestione fornitura per aggiungere un nuovo indirizzo e-mail all'elenco di indirizzi e-mail esistenti e impostare il suddetto in modo che rappresenti l'indirizzo e-mail principale. Tuttavia, l'indirizzo e-mail principale esistente non viene abbassato di livello. Eseguendo tale operazione, l'account può disporre di più indirizzi e-mail principali, i quali non sono consentiti dal sistema nativo. Per evitare ciò, è necessario abbassare di livello l'indirizzo e-mail principale esistente, prima di aggiungerne uno nuovo

Un percorso PKI al file INI troppo lungo può causare il riavvio del server di fornitura

I percorsi UNC che contengono oltre 77 caratteri causano il riavvio del sistema operativo. Per risolvere il problema, evitare di utilizzare percorsi troppo lunghi.

Gli account del PKI appaiono come duplicati

Il connettore PKI non supporta gli endpoint gerarchici di Entrust PKI e archivia tutti gli account in un elenco non ordinato. Per tale motivo, un account univoco di Entrust PKI appare come duplicato al connettore PKI.

Il foglio delle proprietà del gruppo PKI non viene visualizzato correttamente

Quando si tenta di aprire il foglio delle proprietà del gruppo PKI in Gestione fornitura, viene visualizzato un messaggio di errore che indica che non è stato possibile visualizzare il foglio delle proprietà richiesto.

Viene visualizzato un messaggio di notifica e-mail durante la creazione degli account PKI

Se si acquisisce un endpoint PKI utilizzando un profilo proxy ed è attivata la notifica e-mail, non è possibile creare un nuovo account PKI senza specificare l'opzione "Crea profilo".

Per risolvere il problema, attenersi a una delle procedure seguenti:

- Acquisire l'endpoint senza il profilo Proxy.
- Durante l'acquisizione dell'endpoint, disattivare le notifiche di posta elettronica e accedere all'endpoint per verificare manualmente il numero di riferimento

Assegnazione di tipi di utenti contrattuali SAP

Quando si assegna un tipo di utente contrattuale a un utente sulla scheda relativa ai dati della licenza, è possibile apportare le modifiche solo al sistema principale e non ai sistemi secondari.

È possibile modificare i tipi di licenza contrattuale per i sistemi secondari in modo nativo.

Campi obbligatori nell'attributo relativo al tipo di utente contrattuale SAP

Il tipo di utente contrattuale da specificare nella scheda relativa ai dati della licenza dell'account, non può presentare campi obbligatori diversi da LIC_TYPE. Ad esempio, se è necessario specificare il nome del sistema SAP R3 (SYSID) per utilizzare un tipo di utente contrattuale, l'assegnazione avrà esito negativo e verrà visualizzato un messaggio di errore, il quale segnala l'assenza di un valore per il nome del sistema SAP R3.

Il server di connessione C++ può bloccarsi durante una richiesta al connettore PLS

Se il server CCS si è bloccato durante una richiesta al connettore PLS, è necessario controllare l'installazione del server dei criteri, poiché potrebbe rappresentare la causa del problema. Il sintomo che viene rilevato in fase di elaborazione delle richieste sul server dei criteri diminuirà sensibilmente, a causa del costante riavvio del servizio di controllo degli accessi.

Sospensione dell'account SBL

Quando si modifica un account SBL o un modello di account SBL e si sincronizzano le modifiche con un account, si consiglia di non impostare eTSuspended contemporaneamente ad altre modifiche, poiché a causa di tale operazione le altre modifiche apportate all'attributo verrebbero ignorate.

Per risolvere il problema, dividere le richieste in due richieste separate, una contenente le modifiche di eTSuspended e l'altra quelle relative ai valori dei rimanenti attributi.

Messaggi errati durante la verifica della sincronizzazione degli account RSA mediante JIAM

Se durante un'operazione di verifica della sincronizzazione degli account in un account RSA mediante JIAM risulta che l'account manca nell'endpoint, il server di connessione restituisce erroneamente il messaggio di errore: "Lettura del server di connessione non riuscita: errore Sd_GetSerialByLogin - utente non valido", anziché completare correttamente l'operazione e restituire il messaggio "Account mancante nell'endpoint". Verificare che l'operazione di sincronizzazione degli account in Gestione fornitura funzioni correttamente.

La rimozione di più gruppi dall'utente OS/400 causa il blocco di Gestione fornitura

Se si rimuovono più gruppi da un utente in una singola operazione in cui uno o più gruppi iniziano con "#", Gestione fornitura potrebbe non rispondere.

Per risolvere il problema, rimuovere un gruppo alla volta.

Il gruppo primario è stato rimosso dall'account OS/400

L'appartenenza al gruppo OS/400 può essere modificata cambiando l'account che rappresenta un membro del gruppo o cambiando l'appartenenza al gruppo. Quando si modifica l'appartenenza a una dato gruppo, non è possibile rimuovere gli account se questi appartengono a un gruppo primario.

Per risolvere il problema, modificare l'account e rimuovere l'appartenenza al gruppo primario.

Il connettore FND deve contenere entrambe le date "Da" e "A" nell'elenco relativo alle responsabilità

Il connettore FND deve contenere entrambe le date "Da" e "A" nell'elenco relativo alle responsabilità, in caso contrario l'elenco delle responsabilità diviene instabile e non recuperabile.

Per risolvere il problema, è necessario specificare sempre le date "Da" e "A" nell'elenco relativo alle responsabilità, sia durante la creazione o la modifica di un modello di account o un account FND (ad esempio, utilizzando date non recenti o in un lontano futuro, anziché lasciare i vuoti i campi relativi alle date "Da" e "A").

L'icona Host to Caft Definition presente su VISTA non funziona

Se l'agente remoto N16 è stato installato sull'endpoint VISTA o VISTA SP1 e si cerca di aggiungere un server di gestione attraverso Tutti i programmi -> CA -> Identity Manager -> Host to Caft Definition, quindi si tenta l'acquisizione del suddetto computer VISTA come endpoint, viene visualizzato un messaggio di errore che indica che l'accesso è negato.

Per risolvere il problema, aprire il prompt dei comandi e immettere il seguente comando per acquisire l'endpoint.

```
cafthost -a <hostname/IP>
```

Utilizzare percorsi assoluti per accedere a posizioni di ID personalizzati di account LDN e a ID certificato di unità organizzative

L'utilizzo dei percorsi UNC durante l'accesso alle posizioni di ID personalizzati di account LDN e agli ID certificato di unità organizzative, non sempre funziona correttamente con le cartelle condivise in un percorso relativo. Si consiglia di utilizzare un percorso assoluto (inclusa la lettera unità).

La richiesta di ricerca LND in SPML non restituisce alcun risultato

L'esecuzione di una richiesta di ricerca di un account in SPML oppure attraverso il server SPML non restituisce alcun risultato oltre a lastName e homeServer

La correlazione di account LND e utenti globali creati mediante SPML non riesce

In Gestione fornitura, la correlazione di account LND e utenti globali creati mediante SPML, attualmente non riesce

Evitare l'utilizzo di caratteri giapponesi nei nomi account LND

La modifica della password ID attualmente non funziona con gli account contenenti caratteri giapponesi all'interno del nome account. Per risolvere il problema, utilizzare caratteri inglesi nel file ID account.

Impossibile creare account LND con "OU utente univoche"

Non è possibile creare gli account LND con "OU utente univoche". L'account risultante non accessibile e non potrà essere ricercato tramite Gestione fornitura.

L'attributo relativo al nome breve dell'account LND non può contenere più di 85 caratteri giapponesi

L'utilizzo di più di 85 caratteri giapponesi nell'attributo relativo al nome breve dell'account rappresenta, generalmente, la causa dell'arresto del server Domino. Questo problema si verifica solo quando anche il nome dell'account contiene caratteri giapponesi.

Gestione fornitura non visualizza le appartenenze al gruppo dell'account LND, se queste contengono caratteri giapponesi

In Gestione fornitura, gli account creati in Organizzazione e Unità organizzativa che contengono caratteri giapponesi, non vengono visualizzati nelle relative appartenenze al gruppo nella scheda Membro di.

L'account LND e gli ID certificatore contengono caratteri giapponesi non accessibili dal connettore LND JCS

Gli ID certificatore e account contengono caratteri giapponesi non accessibili dal connettore LND JCS. Generalmente tutte le funzioni che richiedono l'accesso a tali file ID, in questa versione non funzionano correttamente.

I caratteri giapponesi nei percorsi DN dell'oggetto LND possono causare problemi durante l'esplorazione

Alcuni caratteri giapponesi nei percorsi DN dell'oggetto, rappresentano generalmente la causa del blocco del Server di fornitura, durante l'esplorazione della directory. Esempi includono: caratteri giapponesi con Unicode 0x80fd, 0x4e88 e 0x5642.

Impossibile rinominare o spostare il connettore LND nella gerarchia sugli account esplorati LND

Questa versione del connettore LND non riesce a eseguire le azioni personalizzate di ridenominazione e spostamento nella gerarchia sugli account esplorati LND. I campi dell'attributo relativo a tali azioni sono disabilitati.

Non esiste alcuna soluzione per tali azioni.

Impossibile eliminare l'account LND e il relativo file di posta utilizzando l'azione personalizzata

L'eliminazione di un account e del relativo file di posta utilizzando l'azione personalizzata non riesce.

Non viene generato alcun messaggio di errore da Gestione fornitura, ma il controllo dell'endpoint mostra che l'account è ancora presente, così come il relativo file di posta. Non esiste alcuna soluzione a tale problema utilizzando Gestione fornitura.

I file di posta dell'account LND non vengono creati durante la registrazione

La finestra di creazione dell'account LND di Gestione fornitura contiene una casella di controllo denominata "Crea repliche", presente sulla pagina della scheda Profilo.

Quando si amministra un endpoint Domino in ambiente cluster e si seleziona la casella di controllo "Crea repliche", vengono create repliche dell'account nell'ambiente cluster, contemporaneamente al file di posta associato. In questa versione, la creazione dei file di posta replicati non viene gestita durante la registrazione.

Capitolo 7: Documentazione

I nomi dei file per le guide di Identity Manager r12 sono i seguenti:

Nome guida	Nome file
Note di rilascio	im_release_enu.pdf
Guida all'implementazione	im_impl_enu.pdf
Guida all'installazione di WebLogic	im_install_weblogic_enu.pdf
Guida all'installazione di WebSphere	im_install_websphere_enu.pdf
Guida all'installazione di JBoss	im_install_jboss_enu.pdf
Guida alla configurazione	im_config_enu.pdf
Guida all'alta disponibilità	im_high_avail_enu.pdf
Guida all'amministrazione	im_admin_enu.pdf
Guida alla programmazione per Java	im_dev_enu.pdf
Guida alla programmazione per la fornitura	im_dev_provisioning_enu.pdf
Guida alla fornitura	im_provisioning_enu.pdf
Guida ai connettori	im_connectors_enu.pdf
Guida a Connector Xpress	im_connector_xpress_enu.pdf
Guida all'implementazione del server di connessione Java	im_jcs_impl_enu.pdf
Guida alla programmazione del server di connessione Java	im_jcsProg_Enu.pdf
Guida all'integrazione di iRecorder	audit_im_irec_ref_enu.pdf
Glossario	im_glossary.pdf
Bookshelf	im_bookshelf_enu.zip

Le seguenti guide di Identity Manager r12 sono disponibili per il download ove indicato di seguito:

- Sito del supporto tecnico di CA

Per visualizzare i file in formato PDF, se non è già installato sul computer, è necessario scaricare ed installare Adobe Reader 7 o versione successiva dal sito Adobe.

Note: per prestazioni ottimali, quando si installa la bookshelf su un sistema remoto, assicurarsi di renderla disponibile da un server Web.

Questa sezione contiene i seguenti argomenti:

Bookshelf

La Bookshelf consente di accedere a tutta la documentazione di Identity Manager da un'unica interfaccia. Include le informazioni seguenti:

- Elenco espandibile dei contenuti di tutte le guide in formato HTML
- Ricerca di testo completa in tutte le guide, con risultati della ricerca classificati e termini di ricerca evidenziati nel contenuto
- Breadcrumb di collegamento ad argomenti di livello superiore
- Un unico indice HTML degli argomenti in tutte le guide
- Collegamenti alle versioni PDF delle guide, destinate alla stampa

Come utilizzare la Bookshelf

1. Scaricare la bookshelf dal sito Web del supporto tecnico di CA.
2. Estrarre i contenuti del file ZIP.
3. Procedere come segue per visualizzare la bookshelf:
   - Se la bookshelf si trova sul sistema locale e viene utilizzato Internet Explorer, aprire il file Bookshelf.hta.
   - Se la bookshelf si trova su un sistema remoto o se viene utilizzato Mozilla Firefox, aprire il file Bookshelf.html.

     Note: per prestazioni ottimali, quando si installa la bookshelf su un sistema remoto, assicurarsi di renderla disponibile da un server Web.

La Bookshelf richiede Internet Explorer 6 o 7 o Mozilla Firefox 2. Per i collegamenti alle guide PDF è richiesto Adobe Reader 7 o 8. Per scaricare Adobe Reader visitare il sito www.adobe.com.

Nota: la Bookshelf di CA SiteMinder è stata pubblicata per r12 e r6.0 SP5 sul sito Web del supporto tecnico di CA con lo stesso formato bookshelf di Identity Manager.

Miglioramenti alla Guida in linea

Le funzioni riportate di seguito sono state aggiunte alla guida in linea della console utente e della console di gestione.

Breadcrumb

Indicano la posizione nella struttura gerarchica della guida per semplificare la navigazione. Si trovano nella parte superiore della pagina della guida.

Evidenziazione delle ricerche

Identifica il contenuto della ricerca nelle pagine risultanti evidenziandolo in giallo.

Pulsanti di navigazione

Pulsanti freccia Precedente e Successivo per semplificare la navigazione. Si trovano nella parte superiore della pagina della guida, sotto i breadcrumb.

Rebranding da eTrust a CA

Il branding di alcuni prodotti di protezione CA è attualmente in transizione da “eTrust” a “CA". In questa fase, nella documentazione potrebbero essere presenti riferimenti a prodotti eTrust e CA. Ad esempio, eTrust Directory diventerà CA Directory nella prossima release. Qualsiasi menzione di un prodotto eTrust nella documentazione è equivalente allo stesso prodotto con il nuovo marchio CA.

Modifiche alla terminologia di fornitura

Gli attuali clienti di eTrust Admin potranno notare alcune modifiche terminologiche con l'integrazione di eTrust Admin in CA Identity Manager. Tali modifiche sono illustrate nella tabella seguente.

Termine in eTrust Admin	Nuovo termine in Identity Manager
Server eTrust Admin	Server di fornitura
eTrust Admin Manager	Gestione fornitura
Directory	Endpoint
Spazio dei nomi	Tipo di endpoint
Criterio o criterio di fornitura	Modello di account
Ruoli	Ruoli di fornitura
Struttura superagenti distribuita	Struttura server di connessione
Superagente	Server di connessione C++
Opzione	Connettore
Directory amministrativa o Repository amministrativo	Directory di fornitura
Directory aziendale di Identity Manager	Archivio utenti di Identity Manager
Utente aziendale	Amministratore in entrata

Nuovo nome per il connettore EIAM (Embedded IAM)

Nella documentazione del prodotto per CA Identity Manager r12, per EEM (Embedded Entitlements Manager) si intende il connettore EIAM (Embedded Identity and Access Manager).

Documentazione di programmazione

La documentazione di Identity Manager r12 comprende due guide alla programmazione.

Guida alla programmazione per Java

Con il titolo precedente di Guida per gli sviluppatori di Identity Manager, fornisce informazioni sull'uso delle API Java di Identity Manager. La versione HTML è integrata con pagine Javadoc e include collegamenti ipertestuali con riferimento alle informazioni pertinenti.

Guida alla programmazione per la fornitura

Con il titolo precedente di eTrust Admin SDK Developer's Guide, questa guida fornisce informazioni sulla programmazione SDK del server di fornitura di Identity Manager. Agli sviluppatori sono richieste conoscenze di programmazione in C++.