CA Identity Manager™

Note di rilascio

12.6.5

Riferimenti ai prodotti CA Technologies

Questo documento è valido per i seguenti prodotti di CA Technologies:

- CA CloudMinder™ Identity Management
- Directory CA
- CA Identity Manager ™
- CA Identity Governance (precedentemente CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

Contattare il servizio di Supporto tecnico

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

Sommario

Capitolo 1: Nuove funzionalità

Questa sezione contiene i seguenti argomenti:

12.6.4

Modifiche apportate alle funzionalità esistenti

CA Identity Manager supporta una nuova versione di CABI

A partire da questa versione, CA Identity Manager supporta soltanto CA Business Intelligence (CABI) versione 3.3 SP1. Il kit di installazione di CA Identity Manager fornisce i programmi di installazione di CABI 3.3 e CABI 3.3 SP1. Per poter installare CABI 3.3 SP1 è necessario installare prima CABI 3.3.

Nuove certificazioni

Le seguenti nuove piattaforme sono certificate con CA Identity Manager r12.6.4:

Endpoint

- CA ControlMinder r12.8 come endpoint
- Windows Server 2012 R2 Active Directory come endpoint
- Database Oracle 12c come endpoint
- Microsoft Lync Server 2010 e 2013 come endpoint
- PeopleSoft Financials 9.2 come endpoint
- System for Cross-domain Identity Management (SCIM) come endpoint
- Lotus Notes Domino 9.x come endpoint

Endpoint dei servizi Web (Layer7)

- Service Now
- Microsoft Azure
- Zendesk

Server applicazioni

- JBoss 6.2.0 EAP

Archivio utenti CA Identity Manager

- Oracle 12c
- Microsoft Windows 2012 R2 Active Directory

Archivio oggetti CA Identity Manager

- Oracle 12c

Provider di credenziali

- Microsoft Windows 8
- Microsoft Windows 8.1

Supporto aggiuntivo

- Supporto dell'agente di sincronizzazione password su Windows Active Directory 2012 R2
- Integrazione con CA SiteMinder r12.52 CR1, r12.52 SP1 e r12.51 CR3
- Supporto browser per IE 11.x
- Supporto browser per Firefox 29.x

Miglioramenti al connettore Top Secret V2 per il supporto di oggetti/attributi aggiuntivi

Il connettore Top Secret V2 è stato migliorato per includere le risorse, le attrezzature, i segmenti e tutti gli altri attributi nel Mainframe.

Miglioramenti apportati alla modifica della password per l'applicazione mobile

L'applicazione mobile dispone di diversi livelli di protezione aggiuntivi per il ripristino della password. Vengono utilizzati sia il metodo PIN che quello Q&A. Per ulteriori informazioni, consultare la *Guida per l'amministratore*.

Miglioramenti apportati al client di caricamento in blocco

Il client di caricamento in blocco è stato migliorato per il supporto delle conversioni Kettle in origini di dati e azioni secondarie. Si tratta di un procedimento simile all'interfaccia utente delle attività in blocco.

Supporto dell'applicazione mobile per sistemi operativi Android

L'applicazione mobile supporta ora le periferiche mobili che utilizzano il sistema operativo Android.

Connector Xpress supporta la personalizzazione di SCIM e del connettore dei servizi Web

Connector Xpress è stato migliorato per il supporto della personalizzazione di SCIM e dei metadati del connettore di servizi Web per

- Service Now
- Azure
- Zendesk

Policy XPress supporta i servizi Web SOAP e REST

Policy XPress è stato migliorato per il supporto SOAP dei servizi Web (con metodo di autenticazione di base) e REST (con metodi di autenticazione di base, autenticazione proxy e autenticazione OAuth). In tal modo, è possibile eseguire l'integrazione con le applicazioni esterne che forniscono l'interfaccia del servizio Web.

Schermata di ricerca Visualizza elenco lavori personali

Una nuova schermata di ricerca è stata aggiunta all'attività Visualizza elenco lavori personali. È pertanto possibile ricercare l'ID utente dell'oggetto del flusso attività o l'iniziatore dell'attività.

12.6.3

Nuove certificazioni

Le seguenti nuove piattaforme sono certificate con CA Identity Manager r12.6.3:

Endpoint

- Microsoft Active Directory Exchange Server 2013 come endpoint
- Salesforce v24 come endpoint
- Solaris 11.1 come endpoint
- SUSE 11 SP3 come endpoint
- CA Directory r12.0 SP12 GA come endpoint Connector Xpress JNDI
- CA ACF2 LDAP r15.1 come endpoint
- CA RACF LDAP r15.1 come endpoint
- CA TSS LDAP r15.1 come endpoint

Sistema operativo del server

- Windows 2012 Essentials

Sistema operativo del client server

- Windows 2012 Essentials
- Windows 8

Server applicazioni

- JBoss 6.1.1 EAP

Archivio utenti CA Identity Manager

- CA Directory r12.0 SP12 GA
- Microsoft Active Directory 2012 Essentials
- Microsoft ADAM 2012 Essentials

Supporto aggiuntivo

- Supporto dell'agente di sincronizzazione password su Active Directory 2012 Essentials
- Internet Explorer 10.x
- Google Chrome 28.x
- Integrazione con CA SiteMinder r12.5 CR3, r12.51 CR1
- Supporto senza agente Unix su RHEL, SUSE, Solaris, AIX e HPUX
- Supporto unicast e multicast con JBoss 6.1.0 EAP
- Supporto di CAM 1.14 con agenti remoti di questa release

- Supporto di AXIS2 1.6.2 con questa release

Supporto unicast per JBoss 6.1 EAP

Per clienti che installano CA Identity Manager su JBoss 6.1 EAP, il protocollo di messaggistica unicast è alternativo al multicast. Si consiglia di sottoporre a test entrambi i protocolli per determinare la scelta migliore per la propria organizzazione.

Per informazioni sull'uso dei due protocolli, consultare la versione dell'*Upgrade Guide* per JBoss.

Generazione di messaggi di posta elettronica e dati di controllo con i nuovi eventi

È possibile abilitare notifiche di posta elettronica e dati di controllo per due nuovi eventi:

- ForgottenPasswordAuditEventQnAInitiated

  L'attività pubblica per le password dimenticate genera questo evento quando un utente consulta la pagina di domanda e risposta durante la reimpostazione della password.

- ForgottenPasswordAuditEventQnALocked

  L'attività pubblica per le password dimenticate genera questo evento quando la pagina di domanda e risposta viene bloccata in seguito ai tentativi non riusciti di rispondere alle domande di sicurezza.

Le notifiche di posta elettronica e il controllo si configurano dalla console di gestione.

Nota: Per informazioni sulla configurazione delle notifiche di posta elettronica, consultare la *Guida per l'amministratore*. Per informazioni sul controllo della configurazione, consultare la *Guida alla configurazione*.

Supporto di ID Vault in Lotus Notes Domino

La funzionalità ID Vault di Lotus Notes Domino è supportata a partire da questa release. Questa funzionalità permette di recuperare e reimpostare password, recuperare ID persi, rinominare utenti e così via, a livello nativo e in modo protetto.

Acquisizione delle informazioni sull'intestazione HTTP

In questa release è stato aggiunto il nuovo filtro di servlet ClientExtractFilter. Questo filtro di servlet sarà fondamentale per estrarre tutte le informazioni relative all'ambiente di client Web. Il filtro permette di estrarre le informazioni dalle intestazioni HTTP. Attualmente viene estratto solo l'indirizzo IP del client. Queste informazioni vengono estratte solo una volta, per la data specificata.

Il filtro di servlet viene eseguito per ciascuna richiesta come suggerito dall'URL pattern:/* in web.xml.

È stata aggiunta la classe di utilità WebClientInformation che funziona come un segnaposto per le informazioni di client Web estratte nel filtro. Questa classe attualmente contiene solo l'indirizzo IP, tuttavia potrebbe essere migliorata in futuro.

La classe WebClientInformation viene inserita in TaskSession come attributo identificato dalla chiave WebClientInfo. In questo modo, qualsiasi evento, attività, interfaccia utente o flusso di lavoro creato in seguito a una richiesta riceverà le informazioni di client dove la richiesta è stata generata.

Miglioramenti degli oggetti di servizio

Nell'attività Elimina utente è stata aggiunta una nuova opzione di casella di controllo, Revoca servizio da utente, per determinare se è necessaria la revoca del servizio prima dell'eliminazione.

È stato aggiunto il supporto del filtro attività Richiedi e visualizza accesso in modo che l'utente abbia la sezione di ricerca per le opzioni di ricerca di amministratore e titolare.

Nell'elemento del flusso di lavoro per l'approvazione della richiesta di servizio ora sono visibili informazioni specifiche della richiesta di servizio, quali la durata e i dati dell'utente. Queste informazioni vengono inviate anche nella notifica di posta elettronica quando è presente un flusso di lavoro basato sul criterio globale configurato sull'evento AddServiceToUserEvent.

12.6.2

Nuove certificazioni

Le seguenti nuove piattaforme sono certificate con CA Identity Manager r12.6.2:

Endpoint

- CA ControlMinder r12.6 SP2 come endpoint
- CA ControlMinder r12.7 come endpoint
- Windows Server 2012 come endpoint NT
- Windows Server 2012 (ADAM) come endpoint JNDI
- CA Directory r12.0 SP11 come endpoint JNDI
- Windows Server 2012 Active Directory come endpoint
- Java Mainframe Connector come endpoint
- Microsoft Active Directory Exchange Server 2010 SP3 come endpoint
- Microsoft Office 365 come endpoint
- SAPJCO V.3 come endpoint

Server applicazioni

- JBoss 6.1 EAP
- WebSphere Application Server (WAS) 8.0
- WebSphere Application Server (WAS) 8.5

Archivio utenti CA Identity Manager

- CA Directory r12.0 SP11 GA

Archivio utenti e archivio oggetti di CA Identity Manager

- Microsoft SQL Server 2008 R2 SP2
- Microsoft SQL Server 2012 SP1

  Nota: JBoss non ha annunciato il supporto per Microsoft SQL Server 2012.

Supporto aggiuntivo

- Java JDK 1.7.x
- Ruoli definiti dall'utente di Microsoft SQL Server 2012 SP1 e ruoli server definiti dall'utente
- Mozilla Firefox 18.x
- Server di rapporto di BusinessObjects XI 3.1 SP6 (CABI 3.3 SP1)
- Integrazione con CA SiteMinder r12.5 CR1, r12.5 CR2, r12.5.1, r12.0 SP3 CR12 e r6 SP6 CR10

- Integrazione con CA Identity Manager, con CA Identity Governance r12.5 SP8 e CA Identity Governance r12.6 SP1
- Supporto app mobili
- Supporto di WorkPoint Designer versione 3.4.2.20080602-33
- Supporto di Microsoft ADS/Exchange modalità senza agente, DAG e distribuzione automatica delle casette postali
- Supporto di CA AuthMinder v7.1

Supporto app mobili

L'applicazione mobile di CA Identity Manager consente di sfruttare l'infrastruttura di CA Identity Manager esistente per permettere agli utenti di completare le attività seguenti in una periferica mobile, come ad esempio un iPhone o iPad:

- Ripristinare una password dimenticata

  Nota: quando si abilitano utenti mobili al ripristino di una password dimenticata dalla loro periferica, CA Identity Manager fa affidamento sulla protezione della periferica, anziché sulle domande di protezione. Prima di abilitare la funzionalità di ripristino della password, considerare la possibilità di richiedere una maggiore protezione della periferica, come ad esempio un codice personale.

- Modificare una password
- Rispondere a richieste di approvazione
- Visualizzare informazioni sul Manager

  Questa funzionalità consente agli utenti che approvano richieste del flusso di lavoro di visualizzare informazioni sul Manager di un utente.

Nota: CA Identity Manager 12.6.5 non supporta la versione 1.0 dell'applicazione mobile. Scaricare l'ultima versione da Apple Store.

Per ulteriori informazioni sull'applicazione mobile, consultare la *Guida per l'amministratore*.

Sincronizzazione/rimozione valori del modello di account dagli account

Ora è possibile utilizzare la funzionalità Sincronizzazione/rimozione valori del modello di account dagli account sull'attributo Elenco Responsabilità di Modello account Oracle Applications per la scadenza di una voce di responsabilità sull'account di Oracle Applications.

Inoltre, questa release comprende miglioramenti nei calcoli della responsabilità per evitare errori di mancata sincronizzazione.

Per ulteriori informazioni sulla funzionalità, consultare la sezione dedicata all'elenco delle responsabilità e alla sincronizzazione degli account nel documento *Connectors Guide*.

Configurazioni migliorate per il connettore LND

Per migliorare le prestazioni del connettore LND durante le operazioni di esplorazione e correlazione, ora sono disponibili le impostazioni configurabili seguenti:

- readExpirationDateInSearch
- readOuFromPrimaryAddressBookOnly
- readAcctFromPrimaryAddressBookOnly
- enableUouDetection

Nota: È possibile modificare i valori degli attributi appena elencati nel file seguente:

```
CA\Identity Manager\Connector Server\conf\override\lnd\connector.xml
```

Schema del database di persistenza delle attività

Questa release comprende miglioramenti agli script SQL che aggiornano lo schema del database di persistenza delle attività. Gli script impostano le dimensioni corrette di colonna e inseriscono la stored procedure denominata Runtime Status Details.

In questo aggiornamento, non vi sono discrepanze di dimensioni fra la tabella runtimeStatusDetail12 e la tabella archive_runtimeStatusDetail12 corrispondente per i sistemi nuovi o aggiornati. Questo aggiornamento elimina gli errori con l'attività Attività di pulitura inoltrate.

Supporto per disattivare la password dell'account SAP

In questa release, l'attributo Password disattivata ora è disponibile nella scheda Account. Con questo attributo è possibile creare un account SAP con una password disattivata. È possibile disattivare anche la password di un account SAP esistente. Reimpostare la password per riattivarla.

Due modalità per la connessione a Exchange: con agente e senza agente

Con questa release è possibile connettersi agli endpoint Exchange 2007 e Exchange 2010 senza agente. Si consiglia di utilizzare la modalità senza agente per le nuove connessioni a questi endpoint.

Tuttavia, la modalità senza agente non funziona con Exchange 2003, pertanto sarà necessario eseguire la connessione mediante un agente remoto.

La tabella seguente elenca le versioni supportate di Exchange per le modalità con e senza agente:

Versioni dell'endpoint	Agente	Senza agente
Exchange 2003	Sì	No
Exchange 2007	Sì	Sì
Exchange 2003 e Exchange 2007	Sì	No
Exchange 2010	Sì	Sì
Exchange 2007 e Exchange 2010	Sì	Sì

Supporto dei gruppi di accesso ai dati (DAG) di Exchange

In questa release, Exchange 2010 può utilizzare gruppi di accesso ai dati (Data Access Group, DAG) ai fini dell'alta disponibilità. È possibile connettersi a un DAG affinché la connessione all'endpoint resti attiva in caso di failover.

Supporto della distribuzione automatica delle casette postali in Exchange 2010

In questa release, il connettore di Active Directory Exchange è in grado di gestire la distribuzione automatica delle casette postali in Exchange 2010.

Quando viene creata o spostata una casella di posta elettronica oppure viene abilitata per un utente esistente, è necessario archiviarla in un database delle cassette postali. Per i server precedenti di Exchange era necessario specificare il database delle cassette postali per eseguire una delle operazioni citate. Invece Exchange Server 2010 seleziona il database mediante la distribuzione automatica delle cassette postali.

Connessione a SQL Server quando il database non è in linea

Ora è possibile esplorare e correlare un endpoint SQL Server quando il database non è in linea.

Attività per creare una definizione snapshot per i rapporti

Ora è consigliabile utilizzare l'attività Crea definizione snapshot per creare una snapshot dei dati necessari per generare un rapporto. I file di parametro XML snapshot predefiniti vengono eliminati gradualmente. Per informazioni, consultare *Guida per l'amministratore*.

12.6.1

Nuove certificazioni

Le seguenti nuove piattaforme sono certificate con CA Identity Manager r12.6.1:

Endpoint

- Microsoft SQL 2012 come endpoint statico e dinamico
- CA Directory r12 SP10 CR2 come endpoint JNDI
- CA Embedded Entitlements Manager (EEM): supportato dal Manager di provisioning

Archivio utenti CA Identity Manager

- CA Directory r12 SP10 CR2

Archivio utenti di CA Identity Manager e archivio di runtime

- Microsoft SQL Server 2012 SP1

Supporto aggiuntivo

- Mozilla Firefox 14.x
- Server di rapporto di BusinessObjects XI 3.1 SP5 (CA Business Intelligence 3.3)

  Questa versione corrisponde alla versione supportata da CA SiteMinder
- Supporto del server di rapporto in una configurazione a disponibilità elevata
- Supporto di CA Identity Manager con CA Identity Governance r12.6
- Supporto di CA Identity Manager con CA SiteMinder r12.0 SP3 CR11

Archivio utenti JNDI abilitato per SSL

La verifica peer dei certificati viene ora applicata. La funzionalità richiede che si aggiunga il certificato del server SSL dell'archivio utenti nel KeyStore attendibile predefinito JRE di CA Identity Manager. Il KeyStore è il file cacerts o jssecacerts in questo percorso:

JAVA_HOME\jre\lib\

Utilizzare il keytool dell'utilità JDK per aggiungere il certificato.

Supporto della crittografia password nella directory di bootstrap della console di gestione

Se la console di gestione è protetta con la directory di bootstrap, detta AuthenticationDirectory, ora è possibile crittografare la password per l'amministratore della console di gestione.

12.6

Nuovo nome e aspetto

La console utente predefinita è stata aggiornata in modo da riflettere i nuovi stili e colori di CA.

Il server di connessione Java (CS Java o JCS) è stato rinominato Server di connessione IAM CA (CA IAM CS).

Esperienza semplificata per gli utenti

Questa versione include i seguenti miglioramenti dell'esperienza per gli utenti:

- Schermate di attività self-service aggiornate

  Le seguenti schermate sono state aggiornate per migliorare la facilità di utilizzo:

  - Aspetto del portale per la schermata di accesso
  - Registrazione automatica e creazione di identità
  - Modifica password personale
  - Reimpostazione password dimenticata
  - ID utente dimenticato

- Alcune attività di amministrazione utilizzano controlli Web 2.0.

Miglioramenti del provisioning

CA Identity Manager 12.6 include le seguenti nuove funzionalità e modifiche per migliorare il provisioning.

Server di provisioning su Linux

Ora è possibile installare il server di provisioning su Red Hat Linux come alternativa a Solaris.

Funzionalità del Manager di provisioning nella console utente

Molte funzionalità del Manager di provisioning vengono ora supportate nella console utente:

- Sincronizzazione di utenti, ruoli, account di endpoint e modelli di account

  L'integrazione di endpoint e account in CA Identity Manager può causare la perdita della sincronizzazione. Ad esempio, i ruoli di provisioning assegnati a un utente possono differire dagli account effettivamente in possesso di tale utente. Le attività di sincronizzazione risolvono questo problema.

- Le regole di correlazione controllano il mapping di attributi degli account di endpoint sugli attributi utente nella console utente. Ad esempio, Access Control ha un attributo chiamato AccountName. È possibile creare una regola per eseguirne il mapping su FullName nella console utente.

Miglioramenti del connettore

CA Identity Manager 12.6 include le seguenti nuove funzionalità e modifiche per semplificare la costruzione e la distribuzione di nuovi connettori.

Distribuzione a caldo: installazione di un nuovo connettore senza la necessità di riavviare CA IAM CS

Il server di connessione IAM CA (CA IAM CS) è il nuovo nome del server di connessione Java (o Java CS o JCS).

CA IAM CS supporta ora la *distribuzione a caldo*. La distribuzione a caldo è il processo di aggiunta, rimozione o aggiornamento di un componente senza la necessità di riavviare CA IAM CS. Ora è possibile effettuare le seguenti attività:

- Installare, disinstallare o eseguire l'aggiornamento di un connettore *senza* la necessità di riavviare CA IAM CS

  È possibile effettuare la distribuzione di un connettore nuovo o aggiornato e installarlo senza la necessità di riavviare CA IAM CS o accedere al suo host. Contattare CA Support per le ultime versioni del connettore.

- Distribuire librerie di terze parti senza la necessità di riavviare CA IAM CS

  Alcuni connettori richiedono librerie che non possono essere fornite con CA IAM CS. In precedenza, sarebbe stato necessario distribuire queste librerie, quindi riavviare CA IAM CS. Ora è possibile distribuire queste librerie mentre il server di connessione è in esecuzione.

  CA IAM CS include un insieme delle principali librerie di terze parti che possono essere utilizzate da qualsiasi connettore. Un connettore può includere anche qualsiasi altra libreria di terze parti necessaria.

Nota: la distribuzione a caldo non funziona per i connettori C++.

Generatore di raggruppamenti: nuovo strumento per la creazione di connettori

CA IAM CS richiede che i connettori vengano forniti come raggruppamento di Open Services Gateway initiative (OSGi). Il framework OSGi è una piattaforma di servizi e sistemi di moduli per il linguaggio di programmazione Java che implementa un modello di componenti completo e dinamico. L'SDK per il server di connessione include ora uno strumento di generazione di raggruppamenti, che aiuta a inserire il connettore in un raggruppamento.

Registrazione per connettori e CA IAM CS

Ora è possibile accedere a CA IAM CS per visualizzare i messaggi di registro recenti per CA IAM CS e i relativi connettori. È comunque possibile utilizzare i file di registro per visualizzare tutti i messaggi di registro.

Certificati per connettori e CA IAM CS

Ora è possibile accedere a CA IAM CS per visualizzare e gestire i certificati per CA IAM CS e i relativi connettori.

Utilizzo di Connector Xpress per eseguire il mapping degli attributi personalizzati e degli attributi di compatibilità personalizzati

Utilizzare Connector Xpress per eseguire il mapping degli attributi personalizzati e degli attributi di compatibilità personalizzati. L'utilizzo del file XML <jcs-home>/conf/override/lnd/lnd_custom_metatdata.xml per eseguire il mapping di attributi non è più possibile.

CA IAM CS è un proxy per CCS

CA Identity Manager utilizza ora CA IAM CS come proxy per il server di connessione C++ (CCS). CA Identity Manager non comunica più direttamente con CCS.

Miglioramenti delle prestazioni

CA Identity Manager 12.6 include miglioramenti delle prestazioni nelle seguenti aree del prodotto.

Miglioramenti delle prestazioni dell'Utilità di caricamento in blocco

In questa versione, le prestazioni dell'Utilità di caricamento in blocco sono state migliorate. I miglioramenti includono le seguenti modifiche:

- Frequenza di inoltro più elevata delle attività attraverso le attività dell'Utilità di caricamento in blocco padre (alimentatore). È possibile eseguire più attività in parallelo.
- Ottimizzazioni nel riutilizzo delle connessioni di database. La memorizzazione in cache delle definizioni di attributo degli oggetti gestiti consente una più rapida esecuzione di ogni attività dall'inizio alla fine.
- Miglioramenti di alcuni plug-in e listener per accelerare l'elaborazione degli eventi generati durante l'esecuzione di attività.

Per migliorare ulteriormente le prestazioni, si consiglia di apportare queste modifiche per l'intera durata dell'operazione di caricamento in blocco:

- Disabilitare eventuali criteri Policy Xpress, gestori attività di logica aziendale e flag di sincronizzazione a livello di attività non desiderati .
- Eseguire l'attività dell'Utilità di caricamento in blocco (alimentatore) come utente dedicato con meno ruoli di amministrazione e attività di amministrazione nell'ambito possibili.

Nota: per ulteriori informazioni su miglioramenti aggiuntivi delle prestazioni, consultare la sezione relativa all'Utilità di caricamento in blocco nella *Guida per l'amministratore*.

Prestazioni di esportazione di snapshot migliorate

In questa versione, sul processo di esportazione di dati di snapshot per i rapporti è stato effettuato il refactoring per migliorare le prestazioni e la facilità di utilizzo. Utilizzando la procedura guidata Definizione snapshot, è possibile definire o personalizzare le regole per caricare utenti, endpoint, ruoli di amministrazione, ruoli di provisioning, gruppi e organizzazioni.

Mediante questa funzionalità, è possibile utilizzare un'attività della console utente per selezionare ed esportare solamente gli attributi desiderati per una determinata istanza di snapshot. Nelle versioni precedenti, gli utenti dovevano modificare manualmente un file XML.

Nota: è comunque possibile utilizzare e personalizzare i file XML predefiniti per l'acquisizione di snapshot.

Per ulteriori informazioni sulla creazione di definizioni snapshot, consultare la *Guida per l'amministratore*.

Miglioramenti di Policy Xpress

Questa versione contiene i seguenti miglioramenti di Policy Xpress:

- Plug-in di attributi per oggetti gestiti

  I seguenti plug-in di attributi degli oggetti gestiti sono stati aggiunti a Policy Xpress:

  - Attributo oggetto: consente di estrarre il valore di qualsiasi attributo di oggetto gestito
  - Presenta un valore di attributo dell'oggetto modificato/Attributo di un oggetto specifico: identici a Presenta un valore di attributo dell'utente modificato e Attributo di un utente specifico, ma funzionano con qualsiasi tipo di oggetto gestito
  - Imposta attributo oggetto: consente di modificare l'attributo di oggetti gestiti

- Funzione Elimina

  La funzione Elimina consente di rimuovere spazi iniziali e finali non richiesti da ciascuna stringa o elemento di dati.

- Supporto per più regole di azione

  In precedenza, quando si tentava di aggiungere più di 60-70 regole di azione a un criterio, Policy Xpress non eseguiva tale azione. In questo caso, nei registri non veniva notificato alcun errore o eccezione. Ora, i criteri di Policy Xpress possono supportare fino a 500 regole di azione.

- Wiki di Policy Xpress

  La documentazione di Policy Xpress è stata aggiornata ed è disponibile nel Wiki della community di utenti globale di CA Security.

Protezione della console di gestione

La console di gestione consente agli amministratori di creare e gestire directory e ambienti di CA Identity Manager.

L'installazione di CA Identity Manager include ora un'opzione, selezionata per impostazione predefinita, per proteggere la console di gestione. Durante l'installazione, si crea un account che può accedere alla console di gestione in una directory predefinita.

Dopo l'installazione, è possibile aggiungere altri amministratori che hanno bisogno dell'accesso alla console di gestione.

Nota: per ulteriori informazioni, consultare la *Guida alla configurazione.*

Richieste di accesso di base

Gli utenti di CA Identity Manager possono richiedere l'accesso ai servizi necessari per l'esecuzione delle loro funzioni lavorative.

Un *servizio* raggruppa insieme tutti i diritti (attività, ruoli, gruppi e attributi) necessari a un utente per un dato ruolo aziendale. I servizi sono disponibili per gli utenti tramite le attività Richiesta di accesso nella console utente di CA Identity Manager. Le attività Richiesta di accesso consentono a un utente o amministratore di richiedere, assegnare, revocare e rinnovare un servizio.

I servizi consentono a un amministratore di associare i diritti dell'utente in un unico pacchetto, che vengono così gestiti come un insieme. Ad esempio, tutti i nuovi dipendenti del reparto Vendite devono accedere a un insieme definito di attività, account su determinati sistemi endpoint. Inoltre, devono aggiungere informazioni specifiche ai loro profili di account utente. Un amministratore crea un servizio denominato Amministrazione vendite, contenente ogni attività, ruolo, gruppo e informazioni di attributo del profilo richiesto per un nuovo dipendente del reparto Vendite. Quando un amministratore assegna il servizio Amministrazione vendite a un utente, costui riceve l'insieme intero di ruoli, attività, gruppi e attributi di account definiti dal servizio.

Un altro modo per gli utenti di accedere ai servizi consiste nel richiedere l'accesso da sé. Nella console utente, ciascun utente dispone di un elenco di servizi disponibili su richiesta. I servizi elencati sono stati contrassegnati dalla voce Sottoscrizione automatica, generalmente impostata da un amministratore con i privilegi appropriati in fase di creazione del servizio. Dall'elenco dei servizi disponibili gli utenti possono richiedere l'accesso ai servizi necessari. Quando l'utente richiede l'accesso a un servizio, la richiesta viene eseguita automaticamente e i diritti associati vengono assegnati immediatamente all'utente. Un amministratore con i privilegi adeguati può configurare, per l'esecuzione di un servizio, la necessità di approvare il flusso di lavoro o la generazione di notifiche di posta elettronica.

Nota: questa versione iniziale supporta capacità di richiesta di accesso di base. La funzionalità Richiesta di accesso consente agli utenti finali di richiedere diritti (gestiti e non gestiti da CA Identity Manager), definire flussi di approvazione e utilizzare flussi di esecuzione.

Questa versione iniziale non fornisce il supporto per le capacità di richiesta di accesso avanzate quali:

- Definizione in blocco di oggetti servizio di richiesta di accesso
- Integrazione con CA Identity Governance (precedentemente chiamato CA GovernanceMinder)
- Filtro e ricerca granulari

Questa versione iniziale non supporta le seguenti capacità:

- Definizione in blocco di oggetti servizio
- Filtro granulare
- Ricerche
- Integrazione con altri meccanismi di esecuzione

Per ulteriori informazioni su tali servizi, consultare la *Guida per l'amministratore*.

Nuova documentazione per Config Xpress

Config Xpress è uno strumento incluso in CA Identity Manager. È possibile utilizzare questo strumento per analizzare e lavorare con le configurazioni dei propri ambienti CA Identity Manager.

Config Xpress consente di eseguire queste attività:

- Spostare i componenti tra gli ambienti.

  Lo strumento individua automaticamente altri eventuali componenti necessari e richiede all'utente anche di spostarli. Questo può risparmiare molte operazioni.

- Pubblicare un rapporto dei componenti di sistema in un file PDF.
- Pubblicare la configurazione XML per un determinato componente.

Per ulteriori informazioni sull'importazione della configurazione, consultare la sezione Gestione della configurazione nella *Guida alla configurazione*.

Sostituzione di CA Identity Manager nativo per SiteMinder Advanced Password Services

Oltre ai criteri di password di base, CA Identity Manager fornisce le seguenti impostazioni aggiuntive per le password ora slegate da SiteMinder:

- Scadenza delle password:
  - Track failed or successful logins (Tieni traccia degli accessi non riusciti o completati): quando quest'impostazione è abilitata, le informazioni di traccia dei tentativi di accesso avvenuti correttamente o non riusciti vengono scritte nell'attributo dati di password dell'utente relativo nell'archivio utenti.
  - Autenticare se impossibile tenere traccia degli accessi: se quest'impostazione è disabilitata, gli utenti non sono in grado di accedere quando CA Identity Manager non può scrivere le informazioni nell'archivio utenti.
  - Password expiration if not changed (Scadenza delle password in caso di mancata modifica): configura il comportamento alla scadenza. Se una password non è stata modificata dopo un determinato numero di giorni, gli utenti vengono disabilitati oppure obbligati a modificare la password. Inoltre, quest'impostazione consente l'invio di avvisi di scadenza per un determinato numero di giorni.
  - Password inactivity (Inattività delle password): configura il comportamento dell'utente inattivo. Se l'utente non ha effettuato un tentativo di accesso corretto dopo un determinato numero di giorni, viene disabilitato oppure obbligato a modificare la password.
  - Password errata: configura il numero di accessi non riusciti consentiti prima che l'utente venga disabilitato.
  - Multiple regular expressions (Più espressioni regolari): specifica espressioni regolari alle quali le password devono o non deve corrispondere. I criteri di password di CA Identity Manager supportano un'espressione singola di ciascun tipo.
- 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: ignora la posizione dei caratteri durante il calcolo della differenza percentuale.

Nota: questa versione non supporta dati di password presenti nella cronologia da una distribuzione di CA Identity Manager che utilizza i servizi di password di CA SiteMinder (cronologia password) a una distribuzione che include solamente i servizi di password di CA Identity Manager r12.6.

Chiavi dinamiche per la crittografia dei dati

In un ambiente, è possibile creare chiavi dinamiche che crittografano o decrittografano i dati. Inoltre, se si suppone che un utente abbia avuto accesso non autorizzato a una chiave, è possibile modificare la password per il KeyStore. KeyStore è il database in cui sono archiviate le chiavi segrete. Una volta modificata la password, CA Identity Manager esegue nuovamente la crittografia dei valori delle chiavi.

La sezione Gestione delle chiavi segrete della *Guida per l'amministratore* contiene ulteriori dettagli.

Sincronizzazione del server Active Directory

È possibile configurare CA IAM CS in modo che consenta agli utenti con server Active Directory (ADS) di sincronizzare informazioni di identità locali con informazioni di endpoint basate su cloud. Ad esempio, potrebbe essere possibile installare ADS per sincronizzarlo con un'installazione di SalesForce basata su cloud. Le aggiunte o le modifiche a un gruppo di utenti locale sincronizzato vengono quindi propagate all'ambiente di SalesForce.

Questa funzionalità richiede CA IAM CS, un endpoint supportato e il connettore appropriato.

Osservare quanto segue sulla funzionalità di sincronizzazione di Active Directory:

- Questa funzionalità supporta solamente Active Directory. Altre directory LDAP non sono supportate per l'uso con questa funzionalità in questa versione.
- Questa funzione supporta solamente endpoint basati su cloud con un connettore esistente. In questa versione, le applicazioni supportate includono Google Apps e SalesForce.

Per ulteriori informazioni su questa funzionalità, consultare la guida *Connectors Guide*.

Verifica degli eventi di accesso e disconnessione

Per migliorare il monitoraggio dell'accesso degli utenti all'ambiente di CA Identity Manager, è possibile configurare CA Identity Manager in modo che verifichi gli eventi di accesso e di disconnessione degli utenti in un ambiente. È possibile visualizzare questi eventi registrati nel rapporto relativo ai dettagli di controllo predefinito.

Nota: non è possibile registrare gli eventi di accesso e di disconnessione degli utenti per CA SiteMinder.

È possibile configurare queste impostazioni nel file di impostazioni di audit. Per ulteriori informazioni sulla configurazione degli eventi di accesso e di disconnessione, consultare il capitolo Controllo nella *Guida alla configurazione*.

Supporto di SHA-2

L'hash dei certificati SSL SHA-2 è un algoritmo crittografico sviluppato dal National Institute of Standards and Technology (NIST) e dalla National Security Agency (NSA). I certificati SHA2 sono più protetti di tutti gli algoritmi precedenti. In CA Identity Manager, è possibile configurare certificati SSL SHA-2 firmati al posto di certificati firmati con la funzione hash SHA-1.

Capitolo 2: Considerazioni sull'installazione

Questa sezione contiene i seguenti argomenti:

Abilitazione del supporto di Policy Xpress per i servizi Web SOAP e REST

Policy XPress è stato migliorato per il supporto SOAP dei servizi Web (con metodo di autenticazione di base) e REST (con metodi di autenticazione di base, autenticazione proxy e autenticazione OAuth). In tal modo, è possibile eseguire l'integrazione con le applicazioni esterne che forniscono l'interfaccia del servizio Web. Per utilizzare i servizi Web di Policy XPress (SOAP e REST) con JBoss 5.1 Community Edition, copiare i seguenti file JAR nella directory \lib\endorsed di JBoss 5.1 Community Edition dalla directory client, quindi riavviare il server applicazioni:

- jbossws-native-jaxrpc.jar
- jbossws-native-jaxws.jar
- jbossws-native-jaxws-ext.jar
- jbossws-native-saaj.jar

Nota: non è necessario effettuare la copia di tali file per le versioni EAP.

Piattaforme e versioni supportate

In CA Identity Manager 12.6.5, sono state apportate modifiche alle versioni del server applicazioni, delle directory e dei database supportati.

Nota: per un elenco completo delle piattaforme e delle versioni supportate, vedere la matrice di supporto di CA Identity Manager sul sito del Supporto tecnico di CA Identity Manager.

Componenti deprecati ed eliminati

Certi componenti vengono deprecati, il che significa che non verranno supportati nelle versioni future. Altri componenti vengono eliminati, nel senso che non verranno più forniti o verificati con il prodotto. Questi componenti sono elencati in CA Identity Manager Deprecation Policy di CA Support.

Installazione simultanea di agenti remoti Unix con altri prodotti CA

In questa release gli agenti remoti UNIX (eccetto per le piattaforme TRU64) ora vengono installati in modo che il software installato tenge traccia dei componenti software dipendenti, come CA ITCM.

Se si desidera aggiornare l'agente remoto UNIX, il nuovo metodo di registrazione non aggiorna il numero di riferimenti dei componenti software dipendenti. Se si desidera disinstallare il prodotto dopo l'aggiornamento, utilizzare il file di disinstallazione seguente:

```
<install-dir>/scripts/uninstall-force.sh
```

Nota: Verificare che uninstall-force.sh non sia utilizzato su host con altri software CA installati. I prodotti possono dipendere dagli stessi pacchetti software rimossi dallo script.

Password non crittografate

Le nuove installazioni non crittografano le password utenti per impostazione predefinita. Inoltre, quando SiteMinder viene integrato con CA Identity Manager, non è possibile abilitare la crittografia delle password utilizzando AttributeLevelEncrypt. Questo attributo funziona solamente quando SiteMinder non è installato.

Questo problema verrà risolto in una versione futura.

Utilizzo di Oracle 11g R2 RAC come archivio utenti e archivio oggetti

Quando si utilizza Oracle 11g R2 RAC come archivio utenti e archivio di runtime, eseguire quanto segue per utilizzare le capacità cluster di un cluster di database Oracle:

- Utilizzare SCAN (Single Client Access Name) mentre si installa CA Identity Manager con Oracle 11g R2 RAC.
- Creare lo *spazio tabella del database* nel gruppo del disco condiviso creando uno spazio tabella.

Oracle 12c RDB come archivio utenti e archivio oggetti

Se si utilizza Oracle 12c RDB come archivio utenti e archivio di runtime, utilizzare soltanto la modalità del database non contenitore. L'opzione RDBMS del database del contenitore di Oracle 12c multi-tenancy è stata esclusa dal prodotto enterprise.

ADAM 2008 come archivio utente

Se si utilizza ADAM 2008 come archivio utente di CA Identity Manager e si integra CA Identity Manager con SiteMinder, è richiesto SiteMinder r6.0 SP6/r6.x QMR6.

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

Durante l'installazione di CA Identity Manager, il programma di installazione estrae i file in una directory temporanea. 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.

Rimedio provvisorio

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

Rimedio provvisorio su Windows 2008 SP2

Durante l'installazione su distribuzioni Windows 2008 SP2, la comunicazione con i componenti di CA Identity Manager, quali il server di fornitura, il server di connessione Java ed il server di connessione C++, è bloccata dal firewall.

Per risolvere questo problema, aggiungere eccezioni alle porte o disabilitare il firewall di Windows per accedere ai componenti distribuiti di CA Identity Manager nelle distribuzioni su Windows 2008 SP2.

Distribuzione di pagine JSP per le azioni dell'amministratore

Il server CA Identity Manager include esempi di pagine JSP per eseguire le azioni seguenti:

- Ping al server applicazioni;
- Elencare BLTH distribuiti;
- Elencare informazioni sui tipi di oggetto e i provider di oggetti gestiti;
- Elencare informazioni sui plugin;
- Modificare i livelli di registrazione.

Le pagine JSP vengono installate in questa posizione:

admin_tools\samples\admin

La cartella di lavoro contiene un file leggimi.txt con istruzioni per l'utilizzo delle pagine JSP.

Nota: se si utilizzano queste pagine JSP senza seguire le istruzioni contenute nel file leggimi verrà visualizzato un errore 404.

Directory di installazione di fornitura su Linux

Se si installa la directory di fornitura su un sistema Linux, il sistema utilizza automaticamente gli indirizzi IPv6 anche se si intende utilizzare IPv4 per il sistema. Tutti i DSA sembrano essere in esecuzione; tuttavia, quando si effettua la connessione ai DSA mediante Jxplorer o si installa il server di fornitura, potrebbe venire visualizzato un messaggio di errore di connessione rifiutata.

Per disattivare IPv6 su Linux

1. Prima di installare la directory di fornitura, attenersi alla procedura indicata nell'articolo di base della conoscenza Red Hat per la Disattivazione di IPv6 su LINUX.
2. Verificare che /etc/hosts non abbia alcuna voce per il seguente indirizzo:

   127.0.0.1 *nome host*

Linux: requisiti di JDK per l'installazione

CA Identity Manager 12.6.5 richiede Oracle JDK 1.6.

RedHat 6.x include OpenJDK 1.6, che può causare un blocco indefinito al programma di installazione di CA Identity Manager. Assicurarsi di utilizzare la versione richiesta di Sun JDK indicata nella Matrice di supporto di CA Identity Manager.

CA Identity Manager su Linux a 64 a bit con errori di connettività a SiteMinder

Il programma di installazione riporta gli errori con CA Identity Manager su Linux a 64 bit quando è selezionata l'opzione Connetti a SiteMinder. La configurazione dell'agente richiesta non è corretta in SiteMinder

Importante: Attenersi alle procedure di rimedio provvisorio prima di distribuire qualsiasi directory o ambiente.

Rimedio provvisorio

1. Annotare il nome agente e la password forniti durante l'installazione. In alternativa, è possibile leggere il valore per la proprietà di AgentName dei seguenti elementi:

   ```
   \iam_im.ear\policyserver.rar\META-INF\ra.xml
   ```

2. Aprire l'interfaccia utente di SiteMinder WAM, quindi creare un agente con il nome agente. Accertarsi di aver selezionato la casella di controllo Agente 4.x.

3. Avviare il server applicazioni e verificare l'esistenza di eventuali problemi di connettività al server dei criteri.

   Verrà visualizzata una riga simile alla seguente senza alcuna eccezione:

   ```
   13:40:43.156 WARN  [valore predefinito] * Fase 2 di avvio : Tentativo di
   avvio di PolicyServerService
   ```

Miglioramento delle prestazioni su WebSphere e AIX

Per un'installazione di WebSphere su AIX, è possibile ottenere migliori prestazioni nella console utente impostando la dimensione heap massima.

Procedere come descritto di seguito:

1. Individuare il file server.xml nel percorso seguente:
   `WAS_HOME/profiles/`*`Profile`*`/config/cells/`*`Cell`*`/nodes/`*`Node`*`/servers/`*`Server`*
2. Aggiungere maximumHeapSize="1000" all'elemento jvmEntries.

   Se necessario, è possibile utilizzare un valore più alto. Ad esempio, per impostare maximumHeapSize su 2 GB (2048 MB), aggiungerlo così come illustrato in grassetto nel seguente estratto da questo file:

```
<jvmEntries xmi:id="JavaVirtualMachine_1183122130078"
verboseModeClass="false"
   verboseModeGarbageCollection="false" maximumHeapSize="2048"
verboseModeJNI="false" runHProf="false" hprofArguments="
debugMode="false" debugArgs="-
agentlib:jdwp=transport=dt_socket,server=y,suspend=n,address=77
77" genericJvmArguments="">
      <systemProperties xmi:id="Property_1"
name="com.ibm.security.jgss.debug" value="off"
required="false"/>
      <systemProperties xmi:id="Property_2"
name="com.ibm.security.krb5.Krb5Debug" value="off"
required="false"/>
    </jvmEntries>
```

Come ignorare l'errore in WebSphere 7/Oracle

Quando CA Identity Manager viene installato utilizzando un archivio di runtime di Oracle e il JRE predefinito di WebSphere 7, nei registri di CA Identity Manager viene visualizzato il seguente errore.

> Oracle does not support the use of version 10 of their JDBC driver with the version of the Java runtime environment that is used by the application server.

Questo errore può essere ignorato.

Capitolo 3: Aggiornamenti

Di seguito vengono descritti i problemi relativi agli aggiornamenti in CA Identity Manager r12.5 SP1.

Questa sezione contiene i seguenti argomenti:

Impostazione dell'ambito del ruolo di amministrazione per il manager di sistema in seguito all'aggiornamento dalla versione 12.6

Durante l'aggiornamento di CA Identity Manager versione 12.6 o successiva, il ruolo di manager di sistema deve essere assegnato all'ambito del ruolo di amministratore.

Nota: se questa operazione non viene eseguita, la ricerca dei ruoli di amministratore potrebbe non restituire alcun risultato.

Eseguire una delle azioni seguenti:

- Nella console di gestione, selezionare Manager di sistema e selezionare un utente.
- In alternativa, è possibile aggiungere l'ambito Ruolo di amministrazione direttamente al ruolo di Manager di sistema utilizzando le opzioni Modifica ruolo di amministrazione, Manager di sistema.

Percorsi di aggiornamento supportati

È possibile eseguire l'aggiornamento a CA Identity Manager 12.6.5 dalle versioni seguenti:

- CA Identity Manager r12
- CA Identity Manager r12.5 o 12.5 SPx
- CA Identity Manager r12.6 o 12.6 SPx

Se si dispone di una versione precedente alla r12 di CA Identity Manager, eseguire innanzitutto l'aggiornamento a r12, r12.5 o r12.5 da SP1 a SP6. Queste versioni includono lo strumento imsconfig, necessario per eseguire l'aggiornamento di una versione precedente alla r12. Quindi, è possibile eseguire l'aggiornamento a CA Identity Manager 12.6.5.

Nuovi script per aggiornare gli schemi di archivio e persistenza delle attività

Questa release include nuovi script per aggiornare gli schemi di archivio e persistenza delle attività. L'aggiornamento viene eseguito automaticamente al primo avvio di CA Identity Manager dopo un aggiornamento. Per ulteriori informazioni sui nuovi script, consultare la *Guida all'installazione*.

Nuovi file JCO per SAP R3

Se si intende utilizzare il nuovo connettore per SAP R3, è necessario aggiornare i file JCO. Per ulteriori informazioni, consultare la guida dell'endpoint per il connettore SAP R3.

Nuovo file di definizione di ruolo di Active Directory

Assicurarsi di importare il nuovo file di definizione di ruolo per Active Directory in ogni ambiente. L'ambiente di CA Identity Manager corrente può avere una versione precedente del file di definizione di ruolo di Active Directory. Quindi, per eseguire l'aggiornamento delle definizioni di ruolo a 1.08, importare il file. Per ulteriori dettagli sull'importazione dei file di definizione di ruolo, seguire le procedure illustrate nella *Guida all'aggiornamento*.

Aggiornamento del file jboss.xml

Durante un riavvio di JBoss o l'inizializzazione di CA Identity Manager, molti messaggi di errore vengono registrati nel file server.log di CA Identity Manager. Questi messaggi sono legati a eventi gestiti da JMX, ma il bean di messaggi ricevente non è stato ancora inizializzato. Per risolvere questo problema, il file seguente include ora una clausola depends:

```
iam_im.ear\iam_im_identityminder_ejb.jar\META-INF\jboss.xml
```

La clausola depends viene inclusa in questa sezione:

```
<message-driven>
<ejb-name>SubscriberMessageEJB</ejb-name>
<destination-jndi-
name>queue/iam/im/jms/queue/com.netegrity.ims.msg.queue
</destination-jndi-name>
<depends>jboss.web.deployment:war=/iam/im</depends>
</message-driven>
```

Assicurarsi di includere questa sezione nel file jboss.xml. Il risultato è che il bean di messaggi ricevente viene inizializzato prima che JMX cominci a elaborare la coda di eventi.

Server applicazioni a 64 bit

CA Identity Manager 12.6.5 supporta server applicazioni a 64 bit, che forniscono prestazioni migliori dei server applicazioni a 32 bit. Sono supportate le seguenti versioni di server applicazioni a 64 bit:

- JBoss 5.0, 5.1 e 6.1 Enterprise Application Platform (EAP)
- JBoss 5.1 Open Source
- Oracle WebLogic 11g (10.3.5)
- IBM WebSphere 7.0, 8.0, 8.5

Per informazioni complete sull'aggiornamento del server applicazioni, consultare l'*Upgrade Guide*.

Problemi durante l'aggiornamento di un cluster da CA Identity Manager r12 CR6 o versioni successive

Se si esegue l'aggiornamento di un cluster da CA Identity Manager r12 CR6 o versioni successive a CA Identity Manager r12.5 SP1, l'aggiornamento potrebbe essere interrotto a causa dell'eliminazione di proprietà cluster nel file di installazione.

Rimedio provvisorio

Verificare che le seguenti proprietà siano contenute nel file di installazione im-installer.properties prima di procedere con l'aggiornamento:

- WebSphere: verificare che il nome del cluster sia presente in DEFAULT_WAS_CLUSTER. In caso contrario, aggiungerlo manualmente.
- WebLogic: verificare che il nome del cluster sia presente in DEFAULT_BEA_CLUSTER. In caso contrario, aggiungerlo manualmente.

Nota: il problema non riguarda il cluster JBoss.

Per impostazione predefinita, il file di installazione si trova nelle seguenti posizioni:

- Windows: C:\Program Files\CA\CA Identity Manager\install_config_info\im-installer.properties
- Unix: /opt/CA/CA_Identity_Manager/install_config_info/im-installer.properties

Errore del flusso di lavoro dopo un aggiornamento da versioni precedenti alla r12.5 SP7

Sintomo:

In caso di aggiornamento da versioni precedenti alla r12.5 SP7 sul server applicazioni di WebLogic, all'avvio del flusso di lavoro viene visualizzato l'errore seguente:

```
AVVISO [ims.default] * Fase di avvio 25: Tentativo di avvio di SchedulerService
in corso
ERRORE [ims.bootstrap.Main] Avvio di FW di IAM non riuscito
ERRORE [ims.bootstrap.Main] org.quartz.SchedulerException: classe JobStore
impossibile configurare le proprietà 'org.quartz.impl.jdbcjobstore.JobStoreCMT'.
[Visualizzare l'eccezione nidificata: java.lang.NoSuchMethodException: Nessun
setter per
la proprietà 'lockHandler.class']
```

Soluzione:

1. Arrestare WebLogic.
2. Passare alla cartella <IAM-EAR>/APP-INF/lib.
3. Rimuovere i seguenti file:
   - common-pool-1.3.jar
   - annotations.jar
   - eurekifyclient.jar
   - quartz-all-1.5.2.jar
4. Avviare il server applicazioni.
5. L'errore di avvio del flusso di lavoro non viene più visualizzato.

Errore di migrazione ambiente

Sintomo:

Se si sta eseguendo l'aggiornamento da CA Identity Manager r12 CR1, CR2, o CR3, è possibile che durante l'importazione degli ambienti venga visualizzato il seguente errore:

L'attributo "accumulateroleeventsenabled" non può essere visualizzato nell'elemento "Provisioning".

Soluzione:

Aprire il file envsettings.xml file nel file esportato Env.zip e modificare accumulateroleeventsenabled in acumulateroleeventsenabled (rimuovere la seconda 'c' in accumulate).

Errore di aggiornamento del provider di credenziali

Dopo l'aggiornamento del provider di credenziali di CA Identity Manager r12 su una piattaforma Windows a 32 bit, la casella di controllo per la disattivazione del provider di credenziali password di Microsoft nell'applicazione CAIMCredProvConfig è deselezionata.

Rimedio provvisorio

Aprire l'applicazione CAIMCredProvConfig e selezionare la casella di controllo.

Errore interno del provider di credenziali Vista

Sintomo:

Quando si esegue l'aggiornamento del provider di credenziali Vista CA Identity Manager su piattaforme Windows a 64 bit, viene visualizzato il messaggio di errore *Errore interno 2324.2.*

Soluzione:

Non è necessaria alcuna azione: il processo di aggiornamento è stato completato correttamente.

Nessuna schermata di ricerca con l'attività Esplora e Correla

Se è stato eseguito l'aggiornamento da CA Identity Manager r12 *o* da CA Identity Manager r12.5 *ed* è stata eseguita la migrazione dell'attività Esplora e Correla al nuovo modello di ricorrenza, il pulsante Sfoglia nell'attività Esplora e Correla non funzionerà correttamente.

Rimedio provvisorio

Configurare una schermata di ricerca per l'attività. In questo modo, facendo clic sul nuovo pulsante Sfoglia, verrà visualizzata una schermata di ricerca.

Errore non irreversibile dopo l'aggiornamento del Manager di provisioning da r12

Sintomo:

Dopo l'aggiornamento del Manager di provisioning da CA Identity Manager r12 CRx, il programma di installazione visualizza un messaggio che segnala che:

```
la procedura guidata ha completato l'aggiornamento di CA Identity
Manager ma si sono verificati errori non irreversibili o avvisi.
Per ulteriori dettagli consultare il registro di installazione in
C:\ programmi\CA\CA Identity Manager.
Avviso/Si sono verificati errori concernenti i seguenti
componenti:
```

Il registro d'installazione di CA Identity Manager contiene la seguente voce:

```
Install, com.installshield.product.actions.Files, err,
ServiceException: (error code = -30016; message = "The process
cannot access the file because it is being used by another
process" (codice errore = -30016; messaggio = "Il processo non può
accedere al file perché è utilizzato da un altro processo")).
```

Soluzione:

L'errore si verifica perché il programma di installazione non è in grado di creare una directory già presente. Tuttavia l'installazione è stata completata e il Manager di provisioning è completamente funzionante.

Come rinominare gli endpoint ACF2, RACF e TSS prima dell'aggiornamento

Gli spazi nei nomi degli endpoint non vengono più supportati. Se sono stati creati endpoint con spazi nel nome in una versione precedente, rimuovere gli spazi prima di eseguire l'aggiornamento a 12.6.

Esecuzione dello script di aggiornamento SQL

Dopo l'aggiornamento, al primo avvio del server di CA Identity Manager viene eseguito uno script. Questo script aggiorna le dimensioni della colonna Descrizione di runtimeStatusDetail12 della tabella Persistenza attività a 2000 caratteri.

In caso di errore dello script, completare i passaggi seguenti:

1. Completare una delle seguenti operazioni:
   - Microsoft SQL Server: aprire lo strumento analizzatore query e selezionare lo script necessario.
   - Oracle: aprire il prompt SQL per lo script necessario.
2. Selezionare uno dei seguenti script:
   - Microsoft SQL Server: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\sqlserver\archive_db_sqlserver_upgrade_to126sp2.sql
   - Oracle su Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\oracle9i\archive_db_oracle_upgrade_to126sp2.sql
   - Oracle su UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/db/taskpersistence/oracle9i/archive_db_derby_upgrade_to126sp2.sql
3. Eseguire il file di script.
4. Verificare l'assenza di errori durante l'esecuzione dello script.

Capitolo 4: Problemi risolti

Questa sezione contiene i seguenti argomenti:

12.6.4

I seguenti problemi sono stati risolti con la versione 12.6.4 di CA Identity Manager:

Ticket di supporto	Problema indicato:
20957471/07	Soluzione necessaria per CQ 170096 su IM 12.6 SP2
21517465/01	Ambito del ruolo di amministrazione nella schermata di ricerca.
21536689/01	La creazione della directory di IM non ricorda la password corretta
21539813/01	Errore di aggiornamento di quote e soglie per gli account LND se l'ACL del file di posta è impostato su Manager
21538682/01	In un IME con token, se il campo di selezione delle date produce un errore, il messaggio di errore restituito mostra l'ID della chiave invece del valore di coppia del raggruppamento delle risorse.
21521403/04	La modifica di un oggetto di servizio comporta la modifica della categoria da Servizio
21547136/01	Per gli account delle applicazioni Oracle, la data di inizio dell'elemento responsibilityList non è visibile per i nuovi account nel Manager di provisioning fino alla nuova esplorazione dell'endpoint, nel caso in cui l'account sia stato creato mediante un modello senza aver definito la data di inizio.
21558292/01	NON CONFORMITÀ 508
20957471/09	Le approvazioni di sincronizzazione inversa vengono generate per rimuovere le responsabilità da un account delle applicazioni Oracle se viene effettuata un'attività di esplorazione dopo la creazione di nuovi account via IM e le responsabilità sono già state assegnate.
21551822/01	risultati erronei di selezione degli oggetti
21567422/01	valore di mapping per l'organizzazione mancante nella Gestione gruppi dopo l'importazione da IM
20957471/11	Comportamento delle policy di account modificate della sincronizzazione inversa diverso da quello previsto per Oracle Server
21576029/01	La descrizione dell'endpoint Windows NT non viene visualizzata nella console utente di IM

21559775/01	Errore di importazione dei ruoli con carattere XML non valido (Unicode: 0x1f) generato dal selettore oggetto nell'attività del ruolo di accesso
21593378/01	Informazioni in tempo reale sulle notifiche del manager non corrette
21590547/01	IM 12.6 SP2: Active Directory- Un attributo vuoto UserPrincipalName comporta errori di mancata sincronizzazione per gli account Active Directory
21588715/01	Quando viene definita una regola di visualizzazione in una schermata di ricerca del ruolo di amministrazione, il filtro di ricerca smette di funzionare.
21590303/01	L'esecuzione della nuova utilità di caricamento in blocco in IM r12.6 SP2 comporta l'apertura di un numero elevato di attività in corso e fa sì che JVM lasci altre richieste in coda.
21594906/01	IM 12.6 SP1 - Errore del livello di audit Entrambi per l'attributo
21574514/02	IM 12.6 SP2: lo stato dell'attività rimane In corso con PX attivato per il flusso di lavoro a livello di evento
21606642/02	tempi di prestazione ridotti per l'attività Modifica membri del gruppo se il gruppo contiene più di 38.000 utenti
21557047/01	Possibili errori del mapping di attributo in Office 365
12345678/01	Nuovo API dell'agente Web SM necessario per IM 12.6 SP4.
21604197/01	L'importazione predefinita del ruolo viene interrotta per il ruolo di provisioning con un nome contenente "\00"
21604199/01	Impossibile effettuare la ricerca dei ruoli di provisioning contenenti il carattere "\" in combinazione con l'asterisco "*".
21609415/01	Errore del connettore Google probabilmente dovuto a un'API non più valida
21626365/01	Errore di script durante la visualizzazione della pagina 2 dei dettagli dell'operazione del manager di provisioning
21613942/01	Modifica del filtro di contenitore dell'account
21419884/02	Le snapshot filtrate eccessivamente richiedono troppo tempo per il completamento
21592259/01	Filtro di password non funzionante per la convalida della password
21640856/01	Quando un'approvazione generata dalla sincronizzazione inversa per aggiungere una responsabilità a un account Oracle Apps viene respinta, la responsabilità non scade anche se viene visualizzata in VST come revocata.
21633958/01	RUOLI DI PROVISIONING DUPLICATI
21641737/01	Livelli di funzionalità Win2012 ADS riportati come Win2008R2
21643258/01	Lo stesso errore riguarda CQ176812. In questo caso, si tratta soltanto di un ordine di lettura
21575724/01	La regola di ambito dell'utente per le policy di amministrazione dei ruoli di amministrazione comporta la mancata visualizzazione dei membri o degli amministratori dopo il riavvio di JBoss
21584724/01	Accesso aggiuntivo per il connettore SAP

21500603/01	Errore dell'integrazione di CA Identity Manager e SiteMinder
21639644/01	Esportazione del modello di account di Oracle
21657577/01	JCS non fa più riferimento a Apache CCPP, pertanto si verificano errori quando JavaScript viene utilizzato con un connettore CXP personalizzato.
21636774/01	Data di fine di responsabilità degli account FND definita sulla data corrente e messaggio ORA/01422: exact fetch returns more than requested number of rows ORA-06512: at "APPS_APPLSYS3.FND_USER_PKG"
21641383/01	L'attività Attiva/Disattiva utente viene interrotta con stato In corso se viene configurato il messaggio di posta elettronica PolXpress.
21646678/01	L'utilità Ant produce un errore durante l'assegnazione dei token ai ruoli se la proprietà Titolo viene aggiunta alle schermate di ricerca.
21657600/01	Errore di importazione da parte di IM dei valori di campo personalizzati per il ruolo di provisioning
21687010/01	Errore di avvio di alcuni rapporti ELM.
21668810/01	Problemi associati all'eliminazione di utenti assegnati a gruppi dinamici.
21699782/01	ELENCO DI ELEMENTO DI LAVORO - LIMITAZIONI. Questo ticket presenta il lavoro necessario per includere gli elementi dell'elenco di lavoro alla pagina facoltativa di accesso.
21650405/01	Lo strumento Config Xpress non carica i flussi di lavoro basati su policy
21539813/01	Le modifiche apportate alla documentazione riguardano la risoluzione del problema PROD00176400.
21712883/01	IM 12.6 SP2 - Gli attributi dell'account Active Directory per la data e l'ora non vengono visualizzati nell'orario locale per la console utente di IM
21669984/01	È possibile utilizzare un'attività privata (non pubblica) chiamata sull'alias pubblico mediante TEWS se IDM e SM sono integrati.
21711390/01	IM 12.6 - Vulnerabilità di protezione- L'URL per la richiesta di una pagina di immagine consente la definizione di contentType da parte di un aggressore. Viene pertanto consentita l'esecuzione del codice nel browser di un utente autenticato che visita l'URL
21713498/01	Lo stato dell'attività viene visualizzato come Completo anche se sono ancora presenti eventi in corso
21699782/01	Ricerca dell'iniziatore e dell'ID utente aggiunta all'elenco di lavoro dell'utente
21704767/01	L'esempio AXIS Java per ModifyGroupMembership.java produce un errore con 12.6 (tutti i Service Pack). Potrebbe essere possibile dover tornare alla versione 12.5
21651991/01	Aggiunta di opzioni di configurazione per l'eliminazione delle notifiche Modify_Account_Password IMPS in IM

21730035/02	IM12.6 SP2: Endpoint Active Directory: Definizione del flag Sarà necessario modificare la password dopo la reimpostazione della scheda Configurazione se l'endpoint non esegue l'aggiornamento del provisioning
21730581/01	Differenze nel tipo di certificazione tra il server di provisioning e l'endpoint LND
21746621/01	Errori di esplorazione/associazione degli account in OU (Unità organizzativa) i cui nomi contengono il carattere "&"
21764131/01	L'attributo singolo di Office365 per le credenziali di blocco viene mappato su eTDYN-str-multi-c/023 invece che su un attributo DYN a valore singolo. Per questo motivo si verificano errori durante la sincronizzazione dell'account con un modello di account WEAK SYNC.

12.6.3

I seguenti problemi vengono risolti in CA Identity Manager 12.6.3:

Ticket di supporto	Problema indicato:
21088049/02	Il processo del flusso di lavoro non risponde nello stato Attivo.
21227662/05	Dopo che un endpoint ACF2 è stato esplorato dall'utente connesso, non è possibile impostare l'utilizzo dell'utente di amministrazione proxy.
21240169/01	StringIndexOutOfBoundsException durante l'esportazione di un ambiente di CA Identity Manager.
21298884/01	Assegnazione/rimozione del servizio da un utente che non esegue la scrittura nell'archivio utenti o l'attivazione di Policy Xpress per gli account.
21325322/03	Impossibile sospendere tutti gli account LND con le sospensioni in blocco o aggiungere tutti gli account al gruppo Rifiuta accesso (Sospeso 0)
21329912/02	La sincronizzazione account non funziona in CA Identity Manager 12.6.
21347968/01 21358148/01	Si è verificato un arresto anomalo del Policy Server quando ruolo di accesso di CA Identity Manager è stato assegnato/rimosso da un utente.
21366658/01	La creazione utenti tramite l'attività dell'utilità di caricamento in blocco restituisce un'eccezione di puntatore null quando CA SiteMinder è integrato.
21378657/01	Il flusso di lavoro di delega a supervisore OOTB viene delegato in modo anomalo se definito utilizzando l'attività Configura il flusso di lavoro basato sul criterio globale per Eventi.
21378803/01	Si verifica un errore di riutilizzo della password precedente e l'attività non viene eseguita.
21385464/01	NullPointerException quando il criterio di identità configurato con MemberRule-Groups Where-Attribute Expression.
21387236/01	La creazione utenti da Copia non esegue la copia dell'attributo dell'organizzazione.
21389685/01	Il tempo per l'accesso aumenta in caso di integrazione con CA SiteMinder.

Ticket di supporto	Problema indicato:
21393295/01	Ruolo di provisioning mancante dall'elenco utenti di CA Identity Manager dei ruoli di provisioning.
21395953/01	Policy Xpress invia cicli di posta.
21417960/01 21417960/03	La modifica del ruolo di provisioning restituisce un puntatore null.
21424762/02	Errore di utente non autorizzato.
21430655/01	Gli eventi del flusso di lavoro basato sul criterio vengono rimandati al responsabile della riassegnazione.
21430868/02	Impossibile rimuovere l'iniziale del secondo nome quando si rinominano gli account LND.
21438148/03	L'organizzazione LND principale non viene esplorata e nessun account viene recuperato.
21438256/01	Lo script java di esempio non funziona con l'attività di registrazione automatica.
21438937/01	Un carattere speciale strano finisce nel valore precedente di persistenza attività e nel controllo.
21439600/01	Il cliente riscontra finestre vuote quando accede con una password utente scaduta.
21441213/01	L'attività di gestione importata dall'ambiente di CA Identity Manager r12.5 restituisce un errore java.lang.ClassCastException.
21447986/01	Quando un criterio di Policy Xpress viene attivato e impostato per l'accesso in lingua norvegese, restituisce l'errore java.lang.IllegalArgumentException: Unmatched braces in the pattern.
21450831/01	Durante l'apertura di un nuovo modello mediante Connector Xpress, non viene mostrata la finestra di dialogo Operation Bindings.
21468616/01	Lunghezza attributo iniziale secondo nome.
21470755/01	Nell'applicazione mobile, la scheda del manager della scheda di contatto non funziona correttamente.
21470794/01	Nell'applicazione mobile, tutti gli errori di reimpostazione password vengono riportati come errori di complessità anche se si inoltra la password corrente errata.
21473825/01	Nell'applicazione mobile di CA Identity Manager, l'accesso non riesce dopo la reimpostazione della password dall'applicazione mobile.
21475033/01	Nell'applicazione mobile di CA Identity Manager, è possibile utilizzare l'attività di reimpostazione della password dimenticata solo una volta.
21478278/01	Un campo CAPTCHA nella schermata CA Identity Manager non viene visualizzato di nuovo quando la fase di convalida rifiuta altri campi.
21480621/01	L'installazione di CA Identity Manager r12.6 SP2 su JBoss EAP 6 non riesce a installare i file iam_im_compile_jsp.* e build.xml.

Ticket di supporto	Problema indicato:
21481343/01	Nessun slot attivo è disponibile poiché vengono bloccati a tempo indeterminato.
21486937/01	Quando il flag di attesa viene controllato per una regola di azione in Policy Xpress per Esegui funzione (non principale) come categoria Codice esterno e tipo Esegui codice Java. L'evento JavaActionWaitEvent viene generato da Policy Xpress e lo stato resta In corso.
21488801/01	La configurazione del criterio di password che richiede segni di interpunzione restituisce una password errata.
21497995/01	Le operazioni in blocco restituiscono un errore quando si seleziona un elemento di elenco di lavoro di delega tra tanti.
21520525/01	Impossibile eseguire <ETAHOME>\bin\ADSLDAPDiag.exe con errore 10054 di lettura dati dal server durante la connessione manuale a un server di Active Directory 2012.
21522674/01	Errore di reimpostazione connessione al passaggio di avvio 5.
21535004/01	Impossibile aggiungere un ruolo SAP con TEWS.
21537907/01	ConfigXpress non funziona nell'installazione di CA Identity Manager r12.6 SP2.
21539251/01	Si verifica un errore durante la creazione di una copia o la modifica dell'attività di amministrazione Visualizza cronologia accessi.
215544431/01	Impossibile creare il criterio del flusso di lavoro globale.
21558358/01	Ricerca di CA CloudMinder/CAFT dell'agente di scambio senza agente in corso
21568224/01	ConfigXpress.air non funziona e restituisce un errore sull'installazione di CA Identity Manager r12.6 SP2.
21572374/01	Nell'applicazione mobile di CA Identity Manager, l'approvazione rapida non funziona.
21585328/01	Impossibile installare ConfigXpress.air su CA Identity Manager r12.6 SP2.

12.6.2

I seguenti problemi vengono risolti in CA Identity Manager 12.6.2:

Ticket di supporto	Problema indicato:
21198613/01	La password impostata con Policy Xpress non è sincronizzata con gli account e l'utente globale.
21230281/01	Impossibile importare i gestori attributo logico nella console di gestione.
21263275/01	Problemi con il criterio di password di Arcot.

Ticket di supporto	Problema indicato:
21269108/02	Problemi con l'installazione dell'agente di sincronizzazione password di CA Identity Manager r12.6.
21264877/01	DN dell'amministratore aggiunto all'URL esterno.
21275958/01	Eccezione puntatore null durante l'acquisizione dell'endpoint SAP.
21272983/01	Errori durante la lettura dell'endpoint di CA Access Control con più database di modello del criterio (PMDB) definiti.
21173122/01	rolesDef importati non visualizzati.
21270763/01	L'errore si verifica con la procedura guidata di creazione di una directory di provisioning.
21280342/01	DoSynchUserRoles non abilita le caselle di controllo Aggiungi account mancanti e Rimuovi account superflui al linguaggio WSDL del servizio Web di esecuzione attività (TEWS) di CA Identity Manager.
21285651/01	Compatibilità con TEWS dell'attività Sincronizza account con modello account.
21295778/01	L'errore durante la creazione di istanze per il plug-in Policy Xpress si verifica durante la creazione o la modifica di un criterio di Policy Xpress.
21304316/01	Problema legato alle prestazioni durante l'aggiunta di gruppi a un utente con attività di creazione o modifica utente.
21304316/02	Problema legato alle prestazioni durante l'aggiunta di gruppi a un utente con il pulsante Aggiungi gruppi sull'attività Modifica utente.
21306987/01	L'errore NoClassDefFoundError si verifica durante l'esecuzione di highavailability.bat.
21307126/01	RSA SecurID 7 - Impossibile acquisire l'endpoint a causa di problemi con lo script per la creazione del pacchetto Open Service Gateway Initiative (OSGi).
21315277/04	Arresto anomalo del server di connessione C++ durante la ricerca di account utente spostati o rinominati di Active Directory.
21319140/01	I dati importati del file dir.xml basati su SQL sono in maiuscolo.
21322022/01	Gli accessi a CA Identity Manager sono più lenti durante un determinato periodo di tempo.
21325322/01	Sessione chiusa a causa di un errore di comunicazione su LND durante la modifica di account.
21331632/01	Il messaggio di avviso durante la revoca del servizio non include il parametro del nome utente.
21335464/01	Errore dello script di gestione provisioning durante la visualizzazione di un'operazione che occupa più pagine.
21351855/01	Impossibile creare con CA Identity Manager un ambiente quando si è scelto solo un ruolo di gestione del sistema senza provisioning.

Ticket di supporto	Problema indicato:
21361599/01 21383034/01	L'errore seguente viene visualizzato quando si utilizza l'attività Modifica utente: Task failed Fatal: Failed to execute SynchronizeAttributesWithAccountEvent: ERRORMESSAGE: For input string
21393461/01	Eccezione durante l'aggiornamento dell'abilitazione/disabilitazione utente o di qualsiasi altro attributo utente.

12.6.1

I seguenti problemi vengono risolti in CA Identity Manager 12.6.1:

Ticket di supporto	Problema indicato:
20576709/02	Deve supportare la condivisione del server di rapporto di BusinessObjects tra CA Identity Manager e SiteMinder
20576725/02	Deve supportare il server di rapporto di BusinessObjects in una configurazione a disponibilità elevata
20583665/02	Deve supportare il server di rapporto di BusinessObjects XI 3.1 SP5 (CABI 3.3)
20774861/02	Impossibile includere dati di oggetti secondari in Policy Xpress
20777137/02	Il miglioramento è stato apportato al flusso di lavoro basato sui criteri affinché ottenga gli oggetti secondari (oggetti dell'utente) necessari per gli oggetti primari
20888199/01	Convenzione di denominazione DN per i modelli di account per TEWS non documentata
21073146/01	Sincronizza account con modello account non effettua la sincronizzazione
21086870/01	Il programma di installazione JCS standalone non richiede la chiave FIPS e causa problemi relativi alla crittografia
21108813/01	CA Identity Manager 12.6 non fornisce le definizioni di ruolo previste
21111634/01	I registri di endpoint JCS non vengono creati
21131768/01	Problema di attributi del flusso di lavoro del criterio globale (alle definizioni di evento mancava il tipo di oggetto secondario)
21135604/01	L'attività View Logical Attribute Handlers (Visualizza gestori attributi logici) non riesce con un errore NullPointer
21136454/01	La vulnerabilità della protezione SQL injection è stata risolta in questa versione
21136456/01	Vulnerabilità della protezione

Ticket di supporto	Problema indicato:
21136499/01	Dati casella di selezione non funziona con una schermata di profilo allegata a un servizio in CA Identity Manager 12.6
21137701/01	Viene ricevuta un'eccezione PxEnvironmentException quando il criterio di Policy Xpress chiama il codice Java esterno
21140501-1	Supporto per le distribuzioni cloud (gestione titolare)
21146621/01	Convalida dell'attributo globale in directory.xml
21156269/01	Differenze fra gli schemi di database generati dal programma di installazione e gli script di database individuali nella cartella degli strumenti
21156269/01	Sono necessari più script per la creazione manuale del database
21162602/01	La correlazione personalizzata per TSS non funziona su Unix
21170706/01	I risultati di Visualizza attività inviate non sono ordinati correttamente quando le impostazioni regionali sono impostate su Danese
21175201/01	La sincronizzazione di account avviata dalla notifica in entrata non avviene quando i ruoli di provisioning vengono assegnati mediante criteri di Policy Xpress
21181592/01	Impossibile caricare CA Identity Manager r12.6 con un errore del percorso di classe non valido
21183366/01	Nome utente errato utilizzato con origini dati
21187385/01	Arresti anomali intermittenti di CA Identity Manager
21188814/01	Il Policy Server di SiteMinder r12 SP3 CR11 si arresta durante l'accesso al criterio di CA Identity Manager
21190699/01	Impossibile ottenere informazioni sugli oggetti secondari da Policy Xpress su criteri basati su eventi o attività. Vengono restituite anche informazioni sui valori di attributo originali anche quando Policy Xpress viene attivato dopo il completamento dell'attività.
21190873/01	Problema di conformità con 508: il suggerimento di strumento delle caselle di controllo non è significativo.
21193837/01	Create&delete Managed Objects (Crea ed elimina oggetti gestiti)
21194712-1	Policy Xpress con l'iteratore si interrompe quando un'assegnazione ruolo di accesso attivata viene rifiutata dal flusso di lavoro
21200396/01	Problema di conformità con 508: problemi con il collegamento Passa al contenuto principale
21200412/01	Problema di conformità con 508: i messaggi di avviso e di errore non vengono letti correttamente dal software di assistenza agli utenti disabili.
21213029-1	Le variabili dei servizi di password archiviate nella cache JSession non vengono cancellate (al momento della disconnessione) e le richieste successive vengono reindirizzate alla pagina pws.fcc

Capitolo 5: Documentazione

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

Nome guida	Nome file
Note di rilascio	im_release_ita.pdf
Guida all'implementazione	im_impl_enu.pdf
Installation Guide for WebLogic	im_install_weblogic_enu.pdf
Installation Guide for WebSphere	im_install_websphere_enu.pdf
Installation Guide for JBoss	im_install_jboss_enu.pdf
Upgrade Guide	im_upgrade_enu.pdf
Configuration Guide	im_config_enu.pdf
Administration Guide	im_admin_enu.pdf
User Console Design Guide	im_uc_design_enu.pdf
Programming Guide for Java	im_dev_enu.pdf
Provisioning Reference Guide	im_provisioning_reference_enu.pdf
Connectors Guide	im_connectors_enu.pdf
Connector Xpress Guide	im_connector_xpress_enu.pdf
Java Connector Server Implementation Guide	im_jcs_impl_enu.pdf
Programming Guide for Java Connector Server	im_jcsProg_Enu.pdf
Glossary	im_glossary.pdf
Bookshelf	im_bookshelf_enu.zip

Questa sezione contiene i seguenti argomenti:

Bookshelf

Il bookshelf consente di accedere a tutta la documentazione di CA 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 per la stampa

Come utilizzare Bookshelf

1. Scaricare la bookshelf dal sito Web del supporto tecnico di CA.
2. Estrarre i contenuti del file ZIP del bookshelf.

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

Per utilizzare Bookshelf è necessario disporre di Internet Explorer 7 o 8 oppure di Mozilla Firefox 2 o 3. Per i collegamenti alle guide PDF è richiesto Adobe Reader 7 o superiore. Per scaricare Adobe Reader visitare il sito www.adobe.com.

Problemi noti

Tutti i problemi noti relativi a CA Identity Manager sono riportati nel sito del Supporto tecnico di CA.

Note di rilascio di integrazione di CA Identity Manager e CA Identity Governance

Tutte le note di rilascio correlate all'integrazione tra CA Identity Manager e CA Identity Governance si trovano nelle *Note di rilascio di CA Identity Governance*. È possibile accedere al bookshelf di CA Identity Governance da CA Support.

Appendice A: Funzionalità di accessibilità

CA Technologies si impegna ad assicurare a tutti i clienti, indipendentemente dalle capacità, la possibilità di utilizzare appieno i propri prodotti e la documentazione di supporto allo scopo di completare operazioni aziendali di importanza vitale. Questa sezione illustra le funzionalità di accessibilità contenute in CA Identity Manager.

Conformità con 508

CA Identity Manager è conforme al paragrafo 508 del Rehabilitation Act e delle Web Content Accessibility Guidelines (WCAG2.0) degli Stati Uniti a livello AA. L'argomento Miglioramenti del prodotto (a pagina 67) fornisce ulteriori dettagli. È anche possibile chiedere al proprio account manager una copia di CA Technology's Voluntary Product Accessibility Template (VPAT).

Miglioramenti di prodotto

CA Identity Manager offre miglioramenti di accessibilità nelle aree seguenti:

- Visualizzazione
- Audio
- Tastiera
- Mouse

Nota: le seguenti informazioni si applicano ad applicazioni basate su Windows e su Macintosh. Le applicazioni Java vengono eseguite su molti sistemi operativi host, alcuni dei quali dispongono già di tecnologie per l'accesso facilitato disponibili. Perché queste tecnologie per l'accesso facilitato forniscano l'accesso a programmi scritti in JPL, hanno bisogno di un bridge tra loro nei loro ambienti nativi e il supporto di accessibilità di Java, disponibile all'interno di Java Virtual Marchine (o Java VM). Questo bridge ha un'estremità in Java VM e l'altra nella piattaforma nativa, e pertanto sarà leggermente diverso per ogni piattaforma per cui funge da bridge. Sun sta attualmente sviluppando sia il JPL, sia le estremità Win32 di questo bridge.

Visualizzazione

Per aumentare la visibilità nello schermo del computer, è possibile regolare le seguenti opzioni:

Font style, color, and size of items (Stile del carattere, colore e dimensione degli elementi)

Consente di scegliere il colore e la dimensione del carattere, nonché altre combinazioni visive.

Screen resolution (Risoluzione dello schermo)

Consente di modificare il numero di pixel per ingrandire gli oggetti nello schermo.

Cursor width and blink rate (Larghezza e velocità di intermittenza del cursore)

Consente di semplificare l'individuazione del cursore o di ridurre al minimo la sua intermittenza.

Icon size (Dimensione delle icone)

Consente di ingrandire le icone per una maggiore visibilità o di ridurle per maggiore spazio nello schermo.

High contrast schemes (Schemi di contrasto alti)

Consente di selezionare combinazioni di colori più facili da visualizzare.

Audio

Utilizzare l'audio come alternativa visiva o per rendere i suoni del computer più facili da sentire o da distinguere regolando le seguenti opzioni:

Volume

Consente di aumentare o diminuire l'audio del computer.

Text-to-Speech (Sintesi vocale)

Consente di sentire le opzioni di comando e il testo letto ad alta voce.

Avvisi

Consente di visualizzare gli avvisi.

Avvisi

Fornisce segnali audio e visivi quando le funzionalità di accessibilità vengono attivate o disattivate.

Schemes (Schemi)

Consente di associare suoni del computer a eventi di sistema specifici.

Captions (Didascalie)

Consente di visualizzare didascalie per testo e suoni.

Nota: se si sta utilizzando un'utilità di lettura dello schermo, si consiglia di installare l'ultima versione per una migliore interpretazione.

Tastiera

È possibile apportare le seguenti modifiche alla tastiera:

Repeat Rate (Velocità di ripetizione)

Consente di impostare la velocità di ripetizione di un carattere quando si preme un tasto.

Tones (Toni)

Consente di sentire toni quando si premono determinati tasti.

Sticky Keys (Tasti permanenti)

Consente a coloro che utilizzano la tastiera con una mano o un dito di scegliere layout di tastiera alternativi.

Skip Link (Ignora collegamento)

Consente di utilizzare il collegamento Passa al contenuto principale per una navigazione rapida al contenuto principale.

Mouse

È possibile utilizzare le seguenti opzioni per rendere il mouse più veloce e più facile da utilizzare:

Click Speed (Velocità doppio clic)

Consente di scegliere la velocità di clic del pulsante del mouse per effettuare una selezione.

Click Lock (Blocca clic)

Consente di selezionare o trascinare senza mantenere premuto il pulsante del mouse.

Reverse Action (Inverti azione)

Consente di invertire le funzioni controllate dai pulsanti sinistro e destro del mouse.

Blink Rate (Velocità di intermittenza del cursore)

Consente di scegliere se e a quale velocità il cursore lampeggia.

Pointer Options (Opzioni puntatore)

Consentono di eseguire le seguenti attività:

- Nascondere il puntatore durante la digitazione
- Mostrare la posizione del puntatore
- Impostare la velocità di movimento del puntatore nello schermo
- Scegliere la dimensione e il colore del puntatore per una maggiore visibilità
- Spostare il puntatore in una posizione predefinita in una finestra di dialogo

Eccezioni di Mozilla Firefox

Si consiglia che gli utenti tastiera e gli utenti JAWS utilizzino Internet Explorer 8 per le ragioni seguenti:

- In Firefox, le finestre di dialogo non ricevono la messa a fuoco/fuori fuoco.
- In Firefox, il collegamento Passa al contenuto principale non sempre viene letto per primo dall'utilità di lettura dello schermo.

Tasti di scelta rapida

La seguente tabella elenca i tasti di scelta rapida supportati da CA Identity Manager:

Tastiera	Descrizione
Ctrl+X	Cut (Taglia)
Ctrl+C	Copia
Ctrl+K	Find Next (Trova successivo)

Tastiera	Descrizione
Ctrl+F	Find and Replace (Trova e sostituisci)
Ctrl+V	Paste (Incolla)
Ctrl+S	Salva
Ctrl+Maiusc+S	Salva tutto
Ctrl+D	Delete Line (Elimina riga)
Ctrl+freccia DESTRA	Next Word (Parola successiva)
Ctrl+freccia GIÙ	Scroll Line Down (Riga giù)
Fine	Fine riga

Riferimenti ai prodotti CA Technologies

Questo documento è valido per i seguenti prodotti di CA Technologies:

- CA CloudMinder™ Identity Management
- Directory CA
- CA Identity Manager ™
- CA Identity Governance (precedentemente CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

Contattare il servizio di Supporto tecnico

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

Capitolo 6: Problemi noti

Questa sezione contiene i seguenti argomenti:

Generale

I problemi riportati di seguito sono problemi noti in CA Identity Manager r12.5 SP1.

Problemi di formattazione tra le visualizzazioni HTML e di testo

Sintomo:

Se viene creato o modificato un messaggio di posta elettronica nell'editor HTML e vengono utilizzate entrambe le visualizzazioni (HTML e di testo), potrebbero verificarsi problemi di formattazione, come ad esempio la modifica dei colori delle tabelle o lo spostamento della tabella stessa. Il problema è stato osservato in Internet Explorer 9 su Windows 7.

Soluzione:

Utilizzare gli altri browser supportati. Per ulteriori informazioni sui browser supportati, consultare la Matrice di supporto della piattaforma di CA Identity Manager r12.6 SP4.

Config Xpress presenta alcune limitazioni durante la migrazione degli oggetti da un ambiente all'altro

Sintomo

Alcuni oggetti, quali Mapping del flusso di lavoro, non possono essere promossi a un altro ambiente mediante Config Xpress.

Soluzione

1. Effettuare l'accesso alla Console utente e accedere a Sistemi, Configura il flusso di lavoro basato sul criterio globale per Eventi.

   Nota: è inoltre possibile accedere a Console di gestione, Impostazioni avanzate, Flusso di lavoro.

2. Eseguire il mapping di un evento su un flusso di lavoro non di modello.

   Nota: l'evento non deve appartenere all'elenco di mapping predefinito.

   Ad esempio, AssignAccessRoleEvent su ModifyAccessRoleMembershipApproveProcess.

3. Esportare il file Environmentsetting.xml da Impostazioni avanzate nella Console di gestione.
4. Eliminare il nuovo mapping aggiunto dall'operazione 2.
5. Importare il file Environmentsetting.xml dell'operazione 3.

   Il mapping creato nell'operazione 2 verrà visualizzato dopo l'importazione.

Errore di domanda/risposta di ripristino del comportamento della password con l'utilizzo delle impostazioni di configurazione della domanda e della risposta predefinite

La domanda/risposta di ripristino del comportamento della password produce un errore con l'utilizzo delle impostazioni di configurazione della domanda e della risposta predefinite nell'amministratore di ambiente delle attività IdentityMinder.

Sintomo

Dopo aver selezionato la domanda e la risposta per il ripristino del comportamento delle password con l'utilizzo delle impostazioni di configurazione della domanda e della risposta predefinite, la password di ripristino produce un errore e comporta la visualizzazione del seguente messaggio:

"ERROR [im.webservices.QuestionAndAnswerResource] (http-/0.0.0.0:8443-1) Failed to process get user credential questions. Message:java.lang.NullPointerException in the server log file"

Soluzione:

Eseguire le seguenti operazioni per attivare il ripristino della password in modo che le domande e le risposte funzionino per il ripristino del comportamento delle password.

Procedere come descritto di seguito:

1. Accedere a Identity Minder come SuperAdmin.
2. Accedere a Attività, Environment Administrator (Amministratore di ambiente), quindi selezionare Configurazione domande e risposte.
3. Fare clic sul pulsante Inoltra.

   Nota: anche i valori predefiniti delle opzioni Attiva e Numero di domande di autenticazione vengono applicati dopo aver eseguito l'operazione.

Il ripristino della password produce un errore dopo l'aggiornamento di IdentityMinder da r12.6 SP2, SP3 a SP4.

Sintomo:

Dopo l'aggiornamento da una delle versioni di CA IdentityMinder r12.6 SP2 o SP3 a 12.6 SP4, il ripristino della password produce un errore in quanto l'opzione Comportamento di reimpostazione password non è impostata su Configurazione mobile.

Soluzione:

Per selezionare manualmente l'opzione Comportamento di reimpostazione password, eseguire le seguenti operazioni.

1. Accedere a Identity Minder come SuperAdmin.
2. Accedere a Attività, Sistema, Configurazione mobile e fare clic su Modifica configurazione mobile.
3. Selezionare la configurazione mobile, quindi accedere alla scheda Funzionalità.
4. Selezionare manualmente una delle opzioni Comportamento di reimpostazione password disponibili.
5. Inoltrare l'attività.

Errore durante la visualizzazione di più servizi

Sintomo:

Quando vengono mostrati più servizi da CA Identity Manager, Axis2 genera una classe stub grande in violazione della regola di compilazione JVM con l'errore seguente:

```
error: code too large for try statement
```

Soluzione:

Quando si riceve questo errore di compilazione, completare i passaggi seguenti ai fini della risoluzione:

1. Aprire il file di classe stub generato dalla directory dei modelli seguente:
   ```
   <samples_dir>\wsdl2java\src\tew6\wsdl
   ```
   Axis2 genera la classe stub nel formato seguente:
   ```
   <Service_name>Stub.java
   ```
   Nota: Recuperare il nome del servizio da WSDL.

2. Nel file di classe stub, suddividere i metodi fromOM e populateFaults. Lo script seguente è un esempio di metodo fromOM dal file di classe stub:
   ```
   public org.apache.xmlbeans.Xmlobject fromOM (
   org.apache.axiom.om.OMElement param,
   java.lang.Class type,
   java.util.Map extraNamespaces) throws
   org.apache.axis2.AxisFault {
   try {
   .......
   .......
   .......
   }catch (java.lang.Exception e) {
   throw org.apache.axis2.AxisFault.makeFault(e);
   }
   return null;
   }
   ```

3. Suddividere lo script di metodo in due metà e nominare l'altra metà, ad esempio, fromOMExtended.

4. Richiamare il metodo appena creato dal metodo di fromOM. Lo script seguente è un esempio del metodo fromOM modificato:
   ```
   public org.apache.xmlbeans.Xmlobject fromOM (
   org.apache.axiom.om.OMElement param,
   java.lang.Class type,
   java.util.Map extraNamespaces) throws
   org.apache.axis2.AxisFault {
   try {
   .......
   .......
   .......
   ```

```
}catch (java.lang.Exception e) {
throw org.apache.axis2.AxisFault.makeFault(e);
}
//invoking the new method
return this. fromOMExtended(param, type, extraNamespaces);
}
```

5. Ripetere i passaggi 3 e 4 per il metodo populateFaults.

6. Salvare le modifiche e immettere il comando seguente dalla posizione della directory dei modelli per compilare le modifiche:

   ```
   sample_dir_location> ant -Dnowsdlgen=true
   ```

   La compilazione non restituisce errori.

Password archiviata in testo non crittografato

Sintomo:

La password per l'utente di bootstrap della console di gestione protetta viene archiviata in testo non crittografato.

Soluzione:

Utilizzare lo strumento di password fornito con il pacchetto di installazione per crittografare la password con l'opzione -JSAFE. Per ulteriori informazioni, consultare la sezione per lo strumento di password nella Guida alla configurazione.

Numero elevato di responsabili dell'approvazione in ApproversList

Sintomo:

Un numero elevato di responsabili dell'approvazione in ApproversList genera l'errore seguente:

```
ORA-12899: Value too large for column error
```

L'attività non viene eseguita e si ha un'interruzione del flusso di lavoro.

Soluzione:

Immettere i seguenti comandi SQL nel database Oracle dove è archiviato il database dei rapporti (archivio oggetti).

```
ALTER TABLE WP_ACT_DATA  MODIFY (VAR_VALUE NVARCHAR2(2000));
ALTER TABLE WP_ACTI_DATA   MODIFY (VAR_VALUE NVARCHAR2(2000));
ALTER TABLE WP_PROC_DATA   MODIFY (VAR_VALUE NVARCHAR2(2000));
ALTER TABLE WP_PROCI_DATA   MODIFY (VAR_VALUE NVARCHAR2(2000));
```

Impossibile connettersi alle pagine Password dimenticata e Sblocca account tramite il provider di credenziali nelle piattaforme Windows 2012 e Windows 8

Windows 2012, come Windows 8, non funziona con il provider di credenziali a causa delle modifiche apportate alla rispettive interfacce da Microsoft

Errore 404 dopo la conferma della reimpostazione password a causa di pws.fcc mancante

Sintomo:

Si utilizza un'attività di IM pubblica chiamata CPSChangeMyPassword in cui l'utente immette la password precedente, quella nuova e richiede la conferma. Dopo aver fatto clic su Invia, quindi su OK per la conferma nella pagina successiva, viene restituito un errore 404, per cui è impossibile trovare il file.

Soluzione:

L'agente Web IIS di SiteMinder 12.5 non contiene il file PWS.fcc nei moduli di directory virtuale IIS. Copiare il file PWS.fcc dalla versione precedente di CA Identity Manager.

Aggiunta di modelli personalizzati di messaggio di posta elettronica per Service Objects

In Service Objects, per ricevere notifiche di posta elettronica e la scadenza del servizio, è necessario creare un modello personalizzato di messaggio di posta elettronica.

Procedere come descritto di seguito:

1. Accedere al seguente percorso:
   `%JBOSS_HOME%\server\default\deploy\iam_im.ear\custom\emailTemplates\default.`
2. Creare un modello personalizzato di messaggio di posta elettronica con nome AddServiceToUserEvent.tmpl nella cartella seguente:
   `iam_im.ear\custom\emailTemplates\default\service_status_folder`
3. Se il servizio è completato o in sospeso, modificare lo stato nella riga 38 di conseguenza.
4. Verificare se la notifica e la scadenza vengono aggiornate nel messaggio di posta elettronica generato.

Errore durante l'installazione di CA Identity Manager con i caratteri UTF-8 nel percorso di installazione o con i dettagli del database in una lingua diversa dall'inglese

Sintomo:

Durante l'installazione di CA Identity Manager 12.6 SP3 con caratteri UTF-8 nel percorso di installazione o con i dettagli del database (nome database, nome utente del database e password database) in una lingua diversa dall'inglese, nei registri di installazione si riscontra l'errore seguente e l'installazione non riesce:

```
C:\Users\Administrator\AppData\Local\Temp\1\598343.tmp\installFrag
ments\dataSource.xml:329: Invalid byte 2 of 4-byte UTF-8 sequence.
```

Soluzione:

Utilizzare caratteri non UTF-8 (testo inglese) nei dettagli del percorso di installazione o del database (nome database, nome utente del database e password database) e procedere con l'installazione nelle seguenti lingue straniere diverse dall'inglese supportate: francese, italiano, tedesco, spagnolo, giapponese, portoghese brasiliano, cinese semplificato, coreano, finlandese, norvegese, svedese, danese e polacco.

Errori di connessione dopo l'aggiornamento del server di CA Identity Minder

Sintomo:

Errore di connessione durante l'accesso a CA Identity Governance da CA Identity Manager dopo l'aggiornamento di un'installazione esistente.

Soluzione:

Dopo l'aggiornamento del server di CA Identity Manager, sono necessarie ulteriori attività di configurazione.

Procedere come descritto di seguito:

1. Nella console utente di CA Identity Manager, accedere a Sistema, Servizi Web, Elimina configurazione dei servizi Web, Cerca.
2. Eliminare la configurazione IMRCM.
3. Accedere al portale Web di CA Identity Governance.
4. Accedere a Amministrazione, Universi e seleziona l'universo configurato per l'integrazione con CA Identity Manager.
5. Accedere alla scheda Connettività e selezionare il connettore di CA Identity Manager.

Fare clic su Verifica e confermare che la connessione è stata eseguita correttamente.

Messaggio di avviso durante l'esecuzione di uno script DDL di snapshot OOTB

Sintomo:

Il seguente script sql genera un indice non valido quando viene eseguito su un database di Microsoft SQL:

`IdentityManager/IAM_Suite/IdentityManager/tools/imrexport/db/SqlServer/ims_mssql_report.sql`

Lo script restituisce il messaggio di avviso seguente:

Warning! The maximum key length is 900 bytes. The index 'imruser6_index_3' has maximum length of 1260 bytes. For some combination of large values, the insert/update operation will fail.

Soluzione:

Procedere come descritto di seguito:

1. Utilizzare il codice seguente per creare una stored procedure:

```
CREATE PROCEDURE sp_imruser6_index_3_exists
AS
BEGIN
DECLARE @MAX_LEN integer
DECLARE @sql_cmd nvarchar(255)
DECLARE @stmt nvarchar(255)
    SET @MAX_LEN = (SELECT SUM(max_length)AS TotalIndexKeySize
FROM sys.columns WHERE name IN (N'imr_userdn', N'imr_reportid')
AND object_id = OBJECT_ID(N'imruser6'))
         IF EXISTS (SELECT name FROM sysindexes WHERE name =
'imruser6_index_3') DROP INDEX imruser6_index_3 on imruser6
    IF (@MAX_LEN > 900)
        CREATE INDEX imruser6_index_3 ON imruser6
(imr_reportid) INCLUDE(imr_userdn)
    ELSE
        CREATE INDEX imruser6_index_3 ON imruser6
(imr_reportid, imr_userdn)
END
GO
```

   La stored procedure è stata creata.

2. Utilizzare il comando seguente per l'esecuzione della stored procedure:

```
EXEC sp_imruser6_index_3_exists
```

Dopo la corretta esecuzione della stored procedure, la colonna che imr_userdn sotto imruser6_index_3 diventa una colonna inclusa.

Guida in linea non sensibile al contesto per l'applicazione mobile

Sintomo:

Quando un utente fa clic sull'icona della guida in linea durante l'esecuzione delle attività delle applicazione mobili, viene visualizzata una guida in linea non correlata.

Soluzione:

Accedere alla guida in linea dell'applicazione mobile dal sommario o tramite una ricerca mirata.

Impossibile creare la directory di provisioning attraverso la console di gestione

Durante la creazione di una directory di provisioning attraverso la console di gestione, il campo nome del dominio server di provisioning non consente caratteri in lingua straniera come nome di dominio. Potrebbe essere visualizzato il seguente messaggio di errore:

"impossibile connettersi al server LDAP machinename:20389 con il DN utente etGlobalUserName=admin,eTGlobalUserContainerName:GlobalUsers,eTNamespacename=CommonObjects,dc=foreignChars, dc=eta e la password specifica."

AttributeLevelEncryption per password utenti

Quando si specifica la classificazione di dati AttributeLevelEncryption per gli attributi nel file di configurazione di directory (directory.xml), CA Identity Manager crittografa il valore attributo nell'archivio utenti. Nella console utente, il valore viene visualizzato non crittografato.

La seguente descrizione dell'attributo mostra la classificazione di dati AttributeLevelEncryption:

```
<ImsManagedObjectAttr physicalname="title" description="Title"
displayname="Title" valuetype="String" maxlength="0"
searchable="false">

<DataClassification name="AttributeLevelEncrypt"/>

</ImsManagedObjectAttr>
```

Negli ambienti con la seguente configurazione, l'abilitazione della crittografia a livello di attributo per le password impedisce agli utenti di accedere:

- CA Identity Manager si integra con CA SiteMinder e
- L'archivio utenti è un database relazionale

In questa versione, la classificazione di dati AttributeLevelEncryption viene rimossa dall'attributo password nel seguente file di configurazione della directory (directory.xml):

- DirectoryTemplates/RelationalDatabase.xml
- fwSampleRDB.xml
- Samples/NeteAutoRDB/NoOrganization.xml
- Samples/NeteAutoRDB/Organization.xml

Questi file si trovano nella directory *admin_tools*:

Nota: per ulteriori informazioni sulla gestione di attributi sensibili, consultare la *Guida alla configurazione*.

Indicazione di DN LDAP quando si utilizza TEWS

Sintomo:

Quando si utilizza TEWS per chiamare l'attività CreateOracleServerAccountTemplate, è possibile che venga restituito il seguente messaggio di errore:

```
Messaggio di errore: <code>500</code>

<description>Impossibile eseguire CreateOracleServerAccountTemplate. ERRORE

MESSAGGIO: com.ca.iam.model.IAMParseException: Gestore IAM non valido:

'UHGUSERS' ProcessStep::Unknown TabName: null ERRORLEVEL::Fatal</description>
```

Il problema è che il valore previsto da DN TEWS non corrisponde al valore nella directory di provisioning.

Questo esempio non funziona correttamente:

```
eTORADirectoryName=WSDLOracle4,eTNamespaceName=Oracle Server,dc=im,dc=eta
```

Questo esempio corrispone al DN non funzionante:

```
EndPoint=WSDLOracle4,Namespace=Oracle Server,Domain=im,Server=Server
```

Soluzione:

Per trovare il mapping, verificare che i livelli di registrazione del server applicazioni vengano impostati su verbose (dettagliato). Eseguire le attività di Identity Manager per cui si richiedono dati/percorsi. I percorsi saranno nei file di registro. L'esecuzione della ricerca in "<" e "insert into IM_" può essere utile per trovare i percorsi e i valori di attributo trasmessi dalle attività.

Errore setpasswd nei sistemi Linux a 64 bit

Sintomo:

Nei sistemi Solaris e Linux a 64 bit, si verifica il seguente errore di setpasswd:

```
"/opt/CA/SharedComponents/csutils/bin/expect: errore durante il caricamento delle
librerie condivise: libtcl8.4.so: non è possibile aprire il file oggetto
condiviso: file o directory non presenti"
```

Soluzione:

Impostare LD_LIBRARY_PATH sul seguente valore:

/opt/CA/SharedComponents/csutils/lib/tcl8.4

setpasswd non genererà più questo errore.

Problema di criterio di password durante l'utilizzo combinato di un archivio utenti e una directory di provisioning

Sintomo:

CA Identity Manager non applica certi criteri di password alle distribuzioni che utilizzano congiuntamente un archivio utenti e directory di provisioning. Questo problema si verifica con criteri di password che includono le seguenti regole e restrizioni:

- Scadenza delle password:
  - Tenere traccia degli accessi non riusciti o completati
  - Autenticazione di un 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.

Questo problema si verifica perché per impostazione predefinita viene eseguito il mapping di %PASSWORD_DATA% su un attributo binario anziché su un attributo stringa.

Soluzione:

Nella console di gestione, eseguire il mapping di %PASSWORD_DATA% su qualsiasi attributo eTCustomField di cui non viene eseguito il mapping su un altro attributo. Ad esempio, eTCustomField99.

Dopo avere aggiornato il mapping, riavviare l'ambiente.

Nota: per ulteriori informazioni sull'aggiornamento di una directory di CA Identity Manager esistente, consultare la *Guida alla configurazione*.

Impossibile connettersi al server di CA IdentityMinder durante la configurazione dell'agente di sincronizzazione password di Active Directory a 64 bit

Sintomo:

Durante la configurazione dell'agente di sincronizzazione password (PSA) a 64 bit, non è possibile connettersi al server di CA Identity Manager per recuperare l'elenco degli endpoint di Active Directory disponibili.

Soluzione:

È possibile configurare solamente le crittografie utilizzate da CA IAM CS. Aggiungere le tre nuove crittografie FIPS SSL alla suite di crittografia utilizzata da CA IAM CS.

Procedere come descritto di seguito:

1. Aprire il seguente file di configurazione in un editor di testo:

   `cs_home\jcs\conf\server_osgi_shared.xml`

2. Individuare nel file la proprietà defaultCipherSuite. Il seguente codice di esempio nel file:

   ```
   <property
   name="defaultCipherSuite"><value>FIPS_TLS_PLUS_SSL_Ciphers</value></property>
   <property name="cipherSuites">
               <map>
                   <entry key="FIPS_TLS_PLUS_SSL_Ciphers">
                       <list>
                           <value>TLS_RSA_WITH_AES_128_CBC_SHA</value>
                           <value>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</value>
                           <value>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</value>
                         </list>
   ```

   In questo esempio, *FIPS_TLS_PLUS_SSL_Ciphers* è la suite predefinita che corrisponde all'elenco di crittografie nella proprietà cipherSuites.

3. Aggiungere le seguenti voci all'elenco:

   ```
   <value>SSL_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA</value>
   ```

4. Fare clic su Salva.

5. Riavviare il servizio CS IAM CA.

   Lo PSA della directory attiva a 64 bit si connette ora senza errori.

Il resolver che partecipa al flusso di lavoro non riesce per EnableUserEventRoles

Sintomo:

Quando si tenta di modificare le impostazioni del flusso di lavoro per l'attività, può essere visualizzato il seguente messaggio:

```
Impossibile impostare il campo "Oggetto primario di questa attività" nella
sezione Descrizione resolver {0} per l'attività di selezione multipla.
```

Soluzione:

Passare alla pagina del flusso di lavoro e modificare il responsabile dell'approvazione in "Oggetto associato all'evento".

Nome duplicato in Visualizza attività inoltrate

Sintomo:

In alcuni ambienti con utilizzo intensivo ed alta disponibilità, il server di CA Identity Manager può inviare richieste simultanee al server di provisioning e introdurre "race condition" nel server di provisioning quando gestisce richieste di modifica parallele sullo stesso utente globale.

Soluzione:

Riavviare il server di provisioning dopo avere selezionato No nella seguente impostazione del Manager di provisioning:

```
server di Identity Manager/Allow Concurrent Modification on Same Global User
(Consenti modifiche simultanee sullo stesso utente globale)
```

Nota: se ci sono utenti globali che possono accedere a Uscita programma, lasciare questo parametro impostato su Sì.

Errore "Not Found" durante la creazione di un nuovo ambiente in alcune distribuzioni

Se CA Identity Manager viene integrato con SiteMinder 6.0.5 CR 31 o versioni successive, quando l'utente prova a ricercare una nuova URL di ambiente viene visualizzato il messaggio di errore "Error 404 - Not found".

Il problema è dovuto a un errore di cache nel server dei criteri.

Rimedio provvisorio

Per risolvere il problema, procedere come segue:

Per Windows:

1. Aggiungere una parola chiave al registro di SiteMinder come descritto di seguito:
   a. Selezionare \\HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\Siteminder\CurrentVersion\ObjectStore
   b. Aggiungere la chiave ServerCmdMsec con le seguenti impostazioni:
      - Tipo: DWORD
      - Valore: 1
   c. Riavviare il server dei criteri
2. Riavviare il server applicazioni.
3. Chiudere tutte le istanze del browser. Utilizzare quindi una nuova istanza del browser per accedere alla URL dell'ambiente.

Per Solaris:

1. Aggiungere una riga al file <CA_HOME folder>/netegrity/siteminder/registry/sm.registry ServerCmdMsec= 0x1 REG_DWORD
2. Riavviare il server dei criteri.
3. Riavviare il server applicazioni.
4. Chiudere tutte le istanze del browser. Utilizzare quindi una nuova istanza del browser per accedere alla URL dell'ambiente.

Modifica di attributi composti a valore singolo in Identity Manager

Se si procede alla modifica di un attributo composto a valore singolo in CA Identity Manager per un endpoint dinamico, specificare solo un valore singolo. Se si specificano valori multipli, il valore esistente viene rimosso e l'attributo rimane senza valore. Il problema non si verifica in Manager fornitura.

Limiti dell'Utilità di caricamento in blocco nel livello attributo di relazione

L'Utilità di caricamento in blocco non può aggiornare le operazioni delle attività negli oggetti dell'utente nel livello attributo di relazione.

- Gli attributi di relazione non aggiornati dall'Utilità di caricamento in blocco sono ruoli di accesso utenti, ruoli di amministrazione utenti, ruoli di provisioning utenti, appartenenza al gruppo Utenti e al gruppo Gruppi.
- Gli attributi di relazione che vengono sovrascritti quando si sostituiscono valori di attributo precedenti con nuovi valori di attributo dal file dell'Utilità di caricamento in blocco sono Amministratori di gruppi e Personalizzato o l'attributo multivalore predefinito.

Errore durante la creazione dell'ambiente con provisioning attivato utilizzando un modello in formato token

In questo caso, CA Identity Manager non può assegnare il ruolo di Manager di sincronizzazione di provisioning all'amministratore in entrata definito nella procedura guidata di creazione dell'ambiente.

Se il modello dell'ambiente comprende token o stringhe tradotte per il nome del ruolo del Manager di provisioning della sincronizzazione, la ricerca non riesce e viene sollevata l'eccezione NoSuchObjectException.

Prerequisito delle applicazioni Oracle

È necessario impostare NLS_LANG come variabile di ambiente di sistema, con .UTF8 come valore.

Nota: nel sistema in cui è installato il server del connettore è necessario un punto (.) prima di UTF8.

archivio utente Oracle 11gR2 RAC: ricerca con distinzione tra maiuscole e minuscole

Sintomo:

Quando Oracle 11gR2 RAC è l'archivio utente, la ricerca di utenti, gruppi o organizzazioni talvolta non fornisce alcun risultato sebbene gli oggetti siano presenti.

Soluzione:

Per l'archivio utente, la ricerca distingue tra maiuscole e minuscole. Ad esempio, la ricerca di *rossi* non produce risultati se l'utente è stato creato come *Rossi* nel database. Utilizzare le stesse maiuscole o minuscole utilizzate al momento della creazione dell'oggetto nel database.

CA Identity Manager su JBoss non si riconnette a Oracle

Sintomo:

Quando si utilizza JBoss 5.x con un'origine dei dati del database Oracle e si effettua l'aggiornamento di CA Identity Manager da una versione r12.5, se il server di database viene riavviato si verifica un'interruzione dell'applicazione. L'interruzione è causata dalla sostituzione da parte di JBoss della proprietà background-validation-minutes con background-validation-millis.

Soluzione:

Per risolvere il problema, attenersi alla seguente procedura:

1. Arrestare il server applicazioni.
2. Aprire i file di origine dati disponibili in */jboss folder/server/default [or server name in cluster]/deploy* ed eliminare la seguente riga:

   <background-validation-minutes> </background-validation-minutes>

3. Aggiungere la seguente riga:

   <background-validation-millis>120000</background-validation-millis>

   Nota: 120000 è l'equivalente di 2 minuti precedentemente specificati per impostazione predefinita per background-validation-minutes. Configurare il valore in base ai requisiti aziendali.

4. Riavviare il server applicazioni.

Nota: il problema non influisce su una nuova installazione di CA Identity Manager.

Collegamento Passa al contenuto principale non riuscito in Mozilla Firefox

Sintomo:

In alto nella console utente, viene visualizzato un collegamento Passa al contenuto principale. Questo collegamento sposta la cornice principale della pagina verso l'alto. Tuttavia, questo collegamento non funziona in Mozilla Firefox.

Soluzione:

Utilizzare Microsoft Internet Explorer 8 o successivo con JAWS per supportare questa funzionalità.

Modifiche simultanee a un utente non riuscite

Un'attività di modifica utente non riesce nelle seguenti situazioni:

- Se si prova a disabilitare un utente durante la sua modifica, l'attività non riesce.
- Se si aggiunge l'attributo forcePasswordChange alla schermata Profilo utente durante la modifica di un utente, l'attività non riesce.

Modifica della sintassi di Policy Xpress

Sintomo:

A causa di una modifica della sintassi di Policy Xpress, potrebbe verificarsi un errore. Questa condizione si verifica se il criterio utilizza l'analisi della stringa per l'ID account e l'utente possiede più account in un endpoint flat. Gli endpoint quali Oracle, OS400 e Microsoft SQL presentano account che fungono da contenitore virtuale, sotto il nome endpoint. A partire dalla versione 12.6.1, la sintassi di un ID account è la seguente:

- Per connettori flat, EndpointName: EndpointName:AccountName
- Per connettori gerarchici, EndpointName:AccountContainerPath:AccountName

Soluzione:

Individuare i criteri di Policy Xpress che utilizzano l'analisi della stringa per l'ID account. Aggiornare tali criteri con la nuova sintassi.

Aggiornamento dell'argomento Guida di SAP

La guida per la scheda predefinita relativa agli account di SAP r3 dovrebbe avere questa definizione per la notazione decimale.

- Consente di specificare i diversi modi di rappresentare la notazione decimale.
- È possibile scegliere fra le opzioni seguenti:

  1.234.567,89

  1,234,567.89

  1 234567,89

Abilitazione della correzione per il bug di Oracle 6376915

Il bug di Oracle 6376915 causa un conflitto per il limite massimo di messa in coda (HW, High Water) quando il database è occupato con la gestione di oggetti di grandi dimensioni (LOB, large objects) e il database è configurato per l'utilizzo della gestione dello spazio dei segmenti automatica (ASSM, Automatic Segment Space Management).

Questo bug provoca problemi di prestazioni e scalabilità con i software di CA, tra cui CA Identity Manager e CA CloudMinder.

La correzione per questo problema comporta un evento obbligatorio. Impostare questo nuovo evento per ottenere un'allocazione più efficiente dei blocchi LOB con l'architettura ASSM.

Questo bug è stato riscontrato a partire da Oracle 10.2.0.3. È stato risolto in Oracle 10.2.0.4 e Oracle 11.1.0.7. Tuttavia, la correzione non è abilitata per impostazione predefinita.

Per i passaggi di questa procedura si prevede che si utilizzi spfile per la configurazione.

Procedere come descritto di seguito:

1. Immettere il comando riportato di seguito:

   ```
   ALTER SYSTEM SET EVENT='44951 TRACE NAME CONTEXT FOREVER, LEVEL
   1024' scope=spfile;
   ```

2. Riavviare il database.
3. Per il test della correzione, svolgere le misurazioni seguenti:
   - Utilizzare l'utilità di caricamento in blocco per misurare la velocità effettiva delle attività in CA Identity Manager e CA CloudMinder.
   - Misurare il tempo di attesa per il conflitto HW enqueue.

Errore di esecuzione dell'attività RequestUserToService

Sintomo:

Quando viene utilizzato Oracle 12c come Objectstore con Jboss 6.x come server applicazioni, viene visualizzato il messaggio di errore "Impossibile eseguire RequestUserToService." ERROR MESSAGE: SmApiWrappedExceptionRA-01843: not a valid month" viene visualizzato nell'interfaccia utenti se un utente effettua la richiesta di un servizio.

Soluzione:

1. Interrompere il server applicazioni Jboss 6.x.
2. Modificare il file denominato **Standalone-full.xml**, disponibile in **<Jboss installed location>\Standalone\Configuration**.
3. Eseguire la ricerca del seguente testo: `jndi-name="java:/iam/im/jdbc/jdbc/objectstore"`.
4. Aggiungere la riga evidenziata visualizzata qui sotto:
```
<datasource jta="false" jndi-name="java:/iam/im/jdbc/jdbc/objectstore" pool-name="iam_im-imobjectstoredb-ds" enabled="true" use-java-context="true">
<connection-url>jdbc:sqlserver://<hostname>:1433;selectMethod=cursor;DatabaseName=<ora_dbname></connection-url>
<driver>sqljdbc</driver>

<new-connection-sql>alter session set NLS_DATE_FORMAT='YYYY-MM-DD' NLS_TIMESTAMP_FORMAT='YYYY-MM-DD HH24:MI:SS.FF3'</new-connection-sql>
```
5. Aggiungere la riga evidenziata visualizzata qui sotto nello stesso file e salvarla.
```
<datasource jta="false" jndi-name="java:/iam/im/jdbc/jdbc/reportsnapshot" pool-name="iam_im-imreportsnapshotdb-ds" enabled="true" use-java-context="true">
<connection-url>jdbc:sqlserver://<hostname>:1433;selectMethod=cursor;DatabaseName=<ora_dbname></connection-url>
<driver>sqljdbc</driver>

<new-connection-sql>alter session set NLS_DATE_FORMAT='YYYY-MM-DD' NLS_TIMESTAMP_FORMAT='YYYY-MM-DD HH24:MI:SS.FF3'</new-connection-sql>
```
6. Avviare il server applicazioni.

Rapporti

Di seguito vengono descritti i problemi relativi ai rapporti in CA Identity Manager r12.5 SP1.

Rapporto Assegna/Revoca ruoli di provisioning - basato su verifica

Sintomo:

Il rapporto Audit - Assegna/Revoca ruoli di provisioning viene generato senza contenere dati se Windows AD 2012 R2 viene utilizzato come archivio utenti.

Soluzione:

1. Accedere alla console di gestione di IdentityMinder.
2. Fare clic su collegamento Ambienti, quindi selezionare <Ambiente AD>.
3. Fare clic su Impostazioni avanzate, Controllo.
4. Fare clic sul pulsante Esporta.
5. Salvare il file xml di Impostazioni audit.
6. Aprire il file xml Impostazioni audit, quindi aggiungere le seguenti righe alla fine del file:
```
<AuditEvent name="RevokeProvisioningRoleEvent" enabled="true"
auditlevel="BOTHCHANGED">
    <AuditProfile objecttype="USER" auditlevel="BOTHCHANGED"/>
    <EventState name="COMPLETE" severity="NONE"/>
    <EventState name="INVALID" severity="CRITICAL"/>
 </AuditEvent>
```
7. Salvare il file.
8. Ripetere le operazioni 1, 2 e 3.
9. Fare clic sul pulsante Importa, selezionare il file xml Impostazioni audit, quindi fare clic sul pulsante Fine.
10. Fare clic su Riavvia ambiente.
11. Generare il rapporto per ottenere un Rapporto Assegna/Revoca ruoli di provisioning - basato su verifica con i dati.

La ricerca con filtro utente prevede la distinzione maiuscole/minuscole nei file XML di snapshot personalizzate degli account di endpoint e degli account utente

Sintomo:

Durante la creazione di un filtro in %USER_ID% in entrambi gli elementi di esportazione *useraccounts* nel file XML di snapshot personalizzate *UserAccounts* e *Endpoint Account*, il rapporto non visualizza i risultati benché l'utente esista.

Soluzione:

La ricerca con filtro prevede la distinzione maiuscole/minuscole.

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).

Problema durante l'utilizzo di più filtri con oggetto endpoint

Sintomo:

Quando viene creata una definizione snapshot con un oggetto endpoint utilizzando più filtri, non viene acquisito alcun dato dell'endpoint.

Soluzione:

Nella scheda Criteri snapshot, anziché selezionare più oggetti endpoint, per selezionare più oggetti endpoint, specificare l'asterisco "*".

La snapshot non acquisisce i dati dell'oggetto gruppo

Sintomo:

Quando viene creata una definizione snapshot con un oggetto gruppo utilizzando org-filter, non viene acquisito alcun dato del gruppo.

Soluzione:

Nella scheda Criteri snapshot, anziché selezionare org-filter dall'elenco a discesa, selezionare (tutti).

Generale

Di seguito vengono riportati problemi di carattere generale relativi alla fornitura in CA Identity Manager r12.5 SP1.

Ridenominazione dei ruoli di provisioning non supportata

La ridenominazione dei ruoli di provisioning dopo la loro creazione non è supportata.

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 mentre il registro viene scritto.

Rimedio provvisorio

Se le prestazioni del server di fornitura non sono soddisfacenti, disattivare la registrazione a ECS.

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 più server di connessione vengono configurati per la gestione di quel dato endpoint. L'errore è dovuto a un problema che si verifica nella fase di eliminazione dell'endpoint, durante la quale non tutti i server di connessione vengono notificati dell'eliminazione dell'endpoint.

Rimedio provvisorio

Riavviare tutti i server di connessione configurati per la gestione dell'endpoint.

La correlazione di un endpoint di Microsoft SQL non riesce

Sintomo:

La correlazione di un endpoint di Microsoft SQL non riesce con il seguente messaggio:
`Creazione dell'oggetto MS SQL Logins (Accessi MS SQL) per gli utenti globali non riuscita. Impossibile determinare la classe oggetto dal nome distinto.`

Questo errore si verifica quando vengono selezionati tutti i contenitori per un endpoint di Microsoft SQL e non solo il contenitore con gli account.

Soluzione:

1. Creare una definizione Esplora e Correla e cercare un endpoint di Microsoft SQL.
2. Cercare tutti i contenitori, ma selezionare solamente il *nome endpoint* come contenitore.
3. Selezionare gli attributi Esplora e Correla.
4. Eseguire la definizione Esplora e Correla.

Restrizioni del nome di accesso a SiteMinder per il nome dell'utente globale

I seguenti caratteri o stringhe di caratteri non possono essere inclusi nel nome di un utente globale se l'utente intende accedere al server dei criteri SiteMinder:

```
&
*
:
()
```

Rimedio provvisorio

Evitare l'utilizzo di tali caratteri nel nome dell'utente globale.

CA IAM CS e Connector Xpress

I seguenti problemi sono relativi al server di connessione IAM CA (CA IAM CS) e a Connector Xpress.

Nota: in CA Identity Manager 12.6, il server di connessione Java (Java CS o JCS) è stato rinominato Server di connessione IAM CA (CA IAM CS).

Schermate di gestione account JNDI - La creazione account con classi oggetto strutturali multiple genera un errore

Non è possibile creare account con classi di oggetti strutturali multipli.

Tipi di endpoint

Di seguito vengono descritti i problemi relativi alla gestione dei tipi endpoint in CA Identity Manager r12.5 SP1.

Generale

Nelle seguenti sessioni vengono descritti i problemi noti relativi a diversi connettori:

Stato account di un account inesistente non visualizzato correttamente nella console utente di CA Identity Manager

Nella console utente di CA Identity Manager, lo stato di un account eliminato in origine non viene visualizzato correttamente. Viene visualizzato un messaggio di operazione riuscita durante la sospensione di un endpoint inesistente.

La configurazione di endpoint con blocco automatico di tentativi richiede un ampio limite di tentativi

Questa sezione si applica a tutti i connettori TSS.

Considerare un endpoint con attivazione del blocco automatico al tentativo N. È necessario configurare l'account utilizzato per la connessione all'endpoint mediante CA IAM CS con un numero N elevato (o illimitato) considerata la velocità con cui CA IAM CS esegue i tentativi di connessione.

Quando l'account viene bloccato a causa del superamento del limite di tentativi N, potrebbe essere necessario utilizzare gli strumenti nativi per sbloccare l'account prima di poter riacquisire l'endpoint. La situazione dipende dall'esatto comportamento di blocco nativo dell'endpoint.

Errore nelle schermate di ricerca di endpoint dopo l'aggiornamento da CA Identity Manager r12.5 SP6 o precedente

Questa sezione si applica a tutti i connettori TSS.

Sintomo:

Un errore che assomiglia al seguente messaggio si verifica quando vengono importati file di definizioni di ruolo di endpoint da r12.5 SP6 o precedente in r12.5 SP7 o successiva:

"Errore nella definizione della schermata "Ricerca compatibilità di endpoint gruppo primario di tipo endpoint predefinito" con tag "DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch" Errore: il tipo "UNKNOWN" non è un tipo di oggetto valido."

In CA Identity Manager r12.5 SP7, alcuni oggetti sono stati rinominati. Nelle schermate di ricerca delle compatibilità dell'endpoint, viene fatto riferimento A questi oggetti. Dopo l'aggiornamento a r12.5 SP7 o versione successiva, è possibile che si verifichi un errore durante l'importazione dei file di definizioni di ruolo che includono schermate con riferimento ai precedenti nomi oggetto.

Questo problema è stato identificato negli endpoint di Active Directory e di CA Access Control.

Soluzione:

Valutare l'opportunità di eliminare le definizioni della schermata che fanno riferimento al nome oggetto precedente prima di importare un file di definizioni di ruolo.

Il caso seguente riguarda un endpoint di Active Directory:

In CA Identity Manager r12.5 SP6, il nome della schermata di ricerca della compatibilità dell'endpoint di Active Directory faceva riferimento all'oggetto ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP.

Il nome oggetto viene visualizzato nella seguente definizione della schermata:

```
<Screen name="Default Active Directory Primary Group Endpoint
Capability Search"
tag="DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

Object="ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP">
```

In CA Identity Manager r12.5 SP7, il nome oggetto è stato modificato in ACTIVEDIRECTORY_ETADSGROUP.

Il nuovo nome oggetto viene visualizzato nella seguente definizione della schermata:

```
<Screen name="Default Active Directory Group Endpoint Capability
Search"

tag="DefaultActiveDirectoryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

object="ACTIVEDIRECTORY_ETADSGROUP">
```

I modelli account non sono sincronizzati con gli account nelle attività Crea o Modifica all'interno della console utente.

Sintomo:

Quando si utilizza questa console, infatti, la sincronizzazione account esplicita non è supportata.

Soluzione:

Utilizzare Manager di provisioning per sincronizzare gli account con i modelli account.

Errore di modifica dell'endpoint durante l'importazione tra l'endpoint ed il server di provisioning.

Questa sezione si applica a tutti i connettori TSS.

Quando l'endpoint viene modificato direttamente senza usare il server di provisioning, viene restituito un errore in fase di importazione. Questo errore deriva dall'incoerenza dei dati tra l'endpoint e il server di provisioning. Di seguito vengono riportati due esempi:

- Un utente ha rimosso delle tabelle dall'endpoint MSSQL utilizzando strumenti nativi e, pertanto, alcuni utenti ricevono risorse non più esistenti.

  Per risolvere l'errore, esplorare nuovamente l'endpoint utilizzando il server di provisioning.

- Alcuni ruoli server sono stati eliminati sull'endpoint. I modelli di account che utilizzavano tali ruoli server ricevevano un numero superiore di ruoli rispetto a quelli esistenti sull'endpoint.

  Per risolvere l'errore, rimuovere manualmente i ruoli server eliminati dai modelli di account.

Restrizione sul nome endpoint per i connettori ACF2 ACFESAGE, RACF IRRDBU00 e TSSCFILE

Sintomo:

Il tentativo di creazione di un endpoint con un nome endpoint quale user test, user-test e _usertest in connettori di file dump impedisce la creazione di endpoint con il messaggio: Impossibile creare factory di connessione abilitata al pool.

Soluzione:

I caratteri di spazio non sono più consentiti in nomi endpoint per i connettori ACF2 ACFESAGE, TSSCFILE RACF o IRRDBU00. Il nome endpoint per questi connettori presenta anche le restrizioni seguenti:

- Deve avere una lunghezza compresa tra 1 e 30 caratteri
- Inizia con caratteri alfanumerici
- Contiene solamente caratteri alfanumerici e/o "_".

Prima di eseguire l'aggiornamento a questa versione, eliminare gli endpoint del file dump mainframe esistenti che non corrispondono alle restrizioni indicate.

CA Access Control

Il testo dei pulsanti della finestra Calendario viene visualizzato in inglese

Durante la creazione di un modello di account nell'endpoint di CA Access Control, i pulsanti OK e ANNULLA nella finestra del calendario vengono visualizzati in inglese nella scheda Accesso.

Rimozione di gruppi da un account di Access Control

Sintomo:

Quando si rimuove un gruppo nativo da un account utente nativo fornito dal connettore di Access Control, i gruppi nativi vengono rimossi in un processo a due fasi. Il processo a due fasi rimuove tutte le appartenenze al gruppo esistenti, quindi aggiunge nuovamente tutte le appartenenze al gruppo richieste. Questo porta all'appartenenza corretta al gruppo per l'account, ma può causare preoccupazioni operative per alcuni clienti.

Soluzione:

Se non si desidera utilizzare il processo a due fasi, è possibile utilizzare Connector XPress per creare una definizione di server di connessione C++ (CCS). La definizione CCS può connettersi direttamente al server di provisioning, anziché essere instradata attraverso CA IAM CS. Questa soluzione alternativa determina una modifica di gruppo a una fase per gli account ACC. Tuttavia, non è possibile utilizzare la console utente per gestire l'appartenenza al gruppo di account ACC. Per gestire l'appartenenza al gruppo di account ACC, utilizzare il Manager di provisioning.

Nota: per informazioni sull'utilizzo di Connector Xpress per creare una definizione di server di connessione C++, consultare How you Set a Managing Connector Server nella *Connector Xpress Guide*.

CA Arcot

Protezione delle attività di ArcotID quando SiteMinder protegge CA Identity Manager

Se SiteMinder protegge CA Identity Manager mediante uno schema di autenticazione CA AuthMinder, le attività seguenti vengono disabilitate in CA Identity Manager:

- Crea/Reimposta ArcotID personale
- Scarica ArcotID personale

Ciò si verifica perché SiteMinder definisce uno schema di autenticazione per una risorsa protetta. Tutte le attività protette di CA Identity Manager hanno lo stesso URL, che viene protetto da uno schema di autenticazione di SiteMinder. Di conseguenza, lo stesso schema di autenticazione copre tutte le attività di CA Identity Manager.

Quando l'autenticazione di ArcotID protegge l'URL di CA Identity Manager, gli utenti devono fornire un ArcotID per l'accesso alle attività. Gli utenti che accedono alle attività sopra riportate non hanno ancora un ArcotID, quindi non possono fornirlo per accedere alle attività.

Per evitare questo problema, utilizzare uno schema di autenticazione diverso da CA AuthMinder quando SiteMinder protegge le attività di CA Identity Manager. Esempi: Active Directory o LDAP.

Nota: Crea/Reimposta ArcotID personale o Scarica ArcotID personale sono attività sensibili. CA Technologies consiglia vivamente di configurare queste attività come attività protette. Se si configurano queste attività come attività pubbliche, gli utenti possono accedervi senza fornire credenziali. Per ulteriori informazioni sulle attività pubbliche, consultare Attività self-service nella User Console Design Guide.

Connettore CA SSO per il server dei criteri avanzati

Nelle seguenti sessioni vengono descritti i problemi noti relativi al connettore CA SSO per il server dei criteri avanzati

Il connettore non può aggiungere più di 2000 conti Profitti e Perdite contemporaneamente ad una applicazione

Non è possibile aggiungere più di 2000 conti Profitti e Perdite ad una applicazione contemporaneamente. Se si desidera aggiungere più di 2000 conti, è necessario suddividere l'operazione in più fasi.

DB2 e DB2 per z/OS

Nelle seguenti sezioni vengono descritti i problemi noti relativi ai connettori DB2 e DB2 per z/OS:

Impossibile salvare un tipo di dati Data a causa della mancata corrispondenza del tipo di dati

Sintomo:

Quando si imposta l'attributo tipo di data in un endpoint DB2 (JDBC DB2 per i IBM), viene visualizzato l'errore seguente:

```
Grammatica SQL errata: il tipo di dati non corrisponde. (YYYY-MM-DD)
```

Soluzione:

Modificare l'URI di connessione nella pagina dell'endpoint in Manager di provisioning e aggiungere *date format=iso*. L'URI finale è il seguente *:jdbc:as400://<host>:CA Portal/<db>;prompt=false;date format=iso;*. Notare lo spazio tra *date* e *format*.

Google Apps

Nelle seguenti sessioni vengono descritti i problemi noti relativi al connettore Google Apps.

Google Apps—Messaggio di errore durante la creazione degli account Google Apps

Sintomo:

Quando creo un account Salesforce.com, visualizzo il seguente messaggio di errore *Failed to Execute CreateGoogleAppsUser Google Apps account has been created, but some additional operation failed (Impossibile eseguire la creazione dell'utente Google Apps. L'utente di Google Apps è stato creato ma si è verificato un errore durante l'esecuzione di un'operazione aggiuntiva)*.

l'account viene creato in CA Identity Manager e nell'endpoint di Google Apps, ma non è visibile nella console utente di CA Identity Manager perché non è associato all'utente globale.

Soluzione:

L'errore si verifica quando si tenta di creare un account con lo stessa combinazione di pseudonimo e nome utente.

per risolvere il problema, eseguire un Esplora e correla nell'endpoint di Google Apps.

L'account creato viene associato all'utente globale in CA Identity Manager ed è ora visibile.

Google Apps—Endpoint Google Apps multipli sullo stesso Java CS

Le impostazioni del connettore Google Apps sono proprietà a livello di sistema. Se si creano due o più endpoint Google Apps sullo stesso Java CS, utilizzare i medesimi server proxy, porta, nome utente e password per tutti gli endpoint Google Apps sullo stesso Java CS.

Google Apps—Messaggio di errore HTTP 403: Forbidden (Accesso negato) visualizzato quando si utilizza l'autenticazione NTLM

Sintomo:

Quando utilizzo l'autenticazione NTLM ricevo l'errore *HTTP 403: Forbidden* (Accesso negato) dal server proxy e il dominio di Google Apps non viene acquisito.

Soluzione:

L'errore si verifica perché in un computer Windows, Java CS viene installato come servizio di Windows e viene eseguito come sistema locale per impostazione predefinita.

Se Java CS è in esecuzione su un computer Windows e NTLM è il più forte schema di autenticazione supportato dal proxy HTTP, il connettore Google Apps tenta di utilizzare l'autenticazione NTLM con il proxy HTTP.

Se il server proxy HTTP in uso utilizza l'autenticazione NTLM, configurare Java CS per l'esecuzione sotto un account di dominio di Windows o un account locale di Windows.

Come configurare l'autenticazione NTLM

Eseguire le operazioni seguenti:

- Eseguire Java CS con un account di Windows che può essere autenticato con il server proxy HTTP senza fornire un nome utente e una password per l'autenticazione proxy durante la creazione dell'endpoint.
- Eseguire Java CS con un account di Windows che non può essere autenticato con il server proxy HTTP, e fornire una combinazione nome utente e password per l'HTTP che può essere autenticata con il proxy durante la creazione dell'endpoint.

Nota: se si utilizza un dominio Windows dell'utente per l'autenticazione del proxy HTTP, anteporre il dominio Windows in cui l'utente si trova al nome utente del proxy HTTP. Ad esempio: DOMINIO\NomeAccountUtenteProxy.

Errore di ricerca di account da Google Apps

Sintomo:

La ricerca di un account Google Apps basato sul nome o sul cognome non riesce.

Soluzione:

L'elaborazione da parte di Google Apps degli aggiornamenti apportati a un nome o cognome utente può richiedere fino a 30 minuti. Per questo motivo, la ricerca del nuovo nome in CA Identity Manager non riesce. Prima di utilizzare il nuovo nome nella ricerca, attendere 30 minuti dopo una modifica di nome.

Microsoft Active Directory e Exchange

I problemi noti per Active Directory e Exchange sono trattati nella *guida all'endpoint per Active Directory e Exchange*. È possibile scaricare la guida dal supporto tecnico di CA.

PeopleSoft

Nelle seguenti sessioni vengono descritti problemi noti relativi al connettore PeopleSoft.

Le ricerche possono non riuscire in Manager di provisioning

Quando si utilizza il Manager di provisioning per cercare un endpoint PeopleSoft con PeopleTools 8.49, la ricerca degli utenti PPS per l'assegnazione dei campi "ID utente alternativo", "ID utente di supervisione" e "Riassegna lavoro a", in alcuni casi non restituisce risultati.

Le soluzioni temporanee possibili sono due:

- utilizzare la console utente di CA Identity Manager per gestire gli endpoint di PeopleSoft (preferibile), oppure
- immettere il valore nei campi del Manager di provisioning senza eseguire le ricerche. Il valore è ancora soggetto a convalida, per cui se il valore immesso non è un utente PPS quando si fa clic sul pulsante Applica l'assegnazione non riesce.

SAP

Nelle seguenti sessioni vengono descritti i problemi noti relativi al connettore SAP

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.

Rimedio provvisorio

È possibile modificare i tipi di licenza contrattuale per i figli.

L'endpoint SAP non viene popolato dal file SAPlogon.in

Quando Manager fornitura è in esecuzione su Windows 2008, i dettagli endpoint per SAP non vengono popolati dal file SAPlogon.ini.

Nota: questo problema è specifico solo per Manager fornitura in esecuzione su Windows 2008.

Rimedio provvisorio

Immettere manualmente i contenuti del file SAPlogon.ini in Manager fornitura.

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.

L'attributo relativo al tipo di utente contrattuale non funziona per tutti i tipi di licenza nella scheda relativa ai dati della licenza account.

Quando il tipo utente viene selezionato dall'elenco disponibile, solo alcuni tipi di utente funzionano. Alcuni tipi di licenza causano un errore di chiamata di funzione 'BAPI', in quanto alcuni tipi di utente contengono campi addizionali non riconosciuti.

Siebel

Nelle seguenti sessioni vengono descritti i problemi noti relativi al connettore Siebel

Errore SBL durante la creazione di account su multipli endpoint

Un modello di account contenente multipli endpoint sarà in grado di elencare solamente gruppi Siebel esistenti su tutti gli endpoint.

Unix v2

Funzionamento diverso delle attività Reimposta password utente per piattaforme varie

Quando un'attività Reimposta password utente viene eseguita in endpoint Suse e HPUX, l'account utente viene abilitato dallo stato Sospeso. Ma, in caso di endpoint RHEL, Solaris e AIX, l'account utente rimane in stato Sospeso.