CA Enterprise Log Manager

Note di rilascio

r12.1 SP1

Riferimenti ai prodotti CA

Questo documento è valido per i seguenti prodotti di CA:

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

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.

Modifiche apportate alla documentazione

Di seguito sono riportati gli aggiornamenti apportati alla documentazione dall'ultimo rilascio.

- Aggiornamento attraverso sottoscrizione - Questo argomento è stato modificato per includere informazioni specifiche per CA Enterprise Log Manager r12.1 SP1. Utilizzare la sottoscrizione per ottenere il Service Pack e per aggiornare CA Enterprise Log Manager per il supporto FIPS.
- Funzionalità nuove o modificate in CA Enterprise Log Manager r12.1 SP1 - Questo capitolo descrive la compatibilità FIPS di CA Enterprise Log Manager, la crittografia utilizzata, i limiti e le modifiche alla configurazione necessarie per accedere all'interfaccia utente da Microsoft Internet Explorer e Mozilla Firefox. Contiene inoltre una sezione sull'utilizzo dell'immagine ISO per nuove distribuzioni e per l'aggiunta di un nuovo server CA Enterprise Log Manager ad una distribuzione esistente.
- Una modifica dell'ora di sistema del server CA EEM genera un errore di non corrispondenza dei certificati - Questo argomento è stato modificato per riflettere la nuova estensione del nome file del certificato .cer.
- Prerequisiti per le impostazioni di risparmio energetico per determinati tipi di computer HP e IBM - Si tratta di un nuovo argomento che descrive le modifiche apportate ai prerequisiti per le impostazioni di risparmio energetico per Server series HP Proliant DL 380G5 e IBM X3650.
- I seguenti problemi noti sono stati rimossi in quanto risolti o non più validi in questo aggiornamento:
  - Agenti non funzionanti con certificati personalizzati
  - Dispatcher syslog secondario non funzionante sotto carico
  - Gli eventi dello stesso host potrebbero visualizzare diversi nomi di host di destinazione
  - Limitazioni alle specifiche dei rapporti PDF
  - Impossibile accedere a CA Enterprise Log Manager dopo l'aggiornamento
  - Visualizzazione incorretta della versione del sensore a seguito dell'aggiornamento diretto alla versione r12.1 M10
  - L'errore "Audit Policy Manager Not installed" ("Gestione del criterio di audit non installata") è incorretto
  - L'interazione con CA Enterprise Log Manager richiede l'aggiornamento a CA Audit.

Ulteriori informazioni:

Sommario

Capitolo 1: Introduzione

Benvenuti in CA Enterprise Log Manager. Il presente documento contiene informazioni relative a sistemi operativi supportati, miglioramenti, problemi noti e procedure per contattare il Supporto tecnico CA.

Aggiornamento attraverso sottoscrizione

Aggiornare CA Enterprise Log Manager all'ultima versione o service pack scaricando tutti i moduli forniti tramite sottoscrizione.

Importante: Aggiornare il server di gestione CA Enterprise Log Manager prima di installare nuovi server CA Enterprise Log Manager nella rete. Seguendo la prassi riportata, i nuovi server potranno essere registrati correttamente.

Seguire queste istruzioni:

1. Controllare la configurazione della sottoscrizione per verificare che la configurazione di base sia completa.
   a. Fare clic sulla scheda Amministrazione, sottoscheda Servizi, e selezionare Modulo di sottoscrizione.
   b. Selezionare No per l'opzione Riavvio automatico dopo l'aggiornamento del sistema operativo.
   c. Spostare il modulo Log Manager nell'elenco selezionato, se l'elenco non è già selezionato.
   d. Verificare che tutti i valori richiesti siano configurati a livello globale.
   e. Verificare che tutti i valori richiesti siano configurati per ciascun server CA Enterprise Log Manager.

   Nota: in ambienti federati, aggiornare gli elementi padre prima dei figli.

   Un evento di automonitoraggio che dichiara che gli aggiornamenti di sottoscrizione sono stati installati indica il completamento dell'operazione.

2. Controllare la configurazione della sottoscrizione per verificare che la configurazione di base sia completa.
   a. Fare clic sulla scheda Amministrazione, sottoscheda Servizi, e selezionare Modulo di sottoscrizione.
   b. Selezionare No per l'opzione Riavvio automatico dopo l'aggiornamento del sistema operativo.
   c. Spostare tutti i moduli restanti per scaricare l'elenco selezionato.

   Nota: in ambienti federati, aggiornare gli elementi padre prima dei figli.
3. Una volta completato il processo di aggiornamento della sottoscrizione, riavviare ciascun server CA Enterprise Log Manager.

   Un evento di automonitoraggio che dichiara che gli aggiornamenti di sottoscrizione sono stati installati indica il completamento dell'operazione.
4. Aggiornare gli agenti e i connettori nel modo seguente:
   a. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri, e infine selezionare Explorer agente.
   b. Determinare se applicare gli aggiornamenti di sottoscrizione a livello di Explorer agente, di gruppo agenti o di singolo agente.
   c. Selezionare il livello desiderato e fare clic sul pulsante Sottoscrizione.
   d. Applicare gli aggiornamenti agli agenti se Agenti era tra i moduli scaricati.
   e. Fare nuovamente clic sul pulsante Sottoscrizione.
   f. Applicare gli aggiornamenti ai connettori, quando disponibili.
5. Eseguire nuovamente la registrazione dei prodotti di terze parti e di altri prodotti CA, come CA Access Control, che visualizzano i rapporti CA Enterprise Log Manager nelle rispettive interfacce native utilizzando chiamate Open API.

   In tal modo, sarà possibile aggiornare i certificati modificati in questa versione. Per ulteriori informazioni, consultare la *Guida alla programmazione API di CA Enterprise Log Manager*.

Nota: per problemi noti relativi agli aggiornamenti della sottoscrizione, consultare le Note di rilascio.

Ulteriori informazioni:

Riavvio automatico dopo l'aggiornamento del sistema operativo durante l'aggiornamento del Service Pack (a pagina 63)
L'aggiornamento del sensore log syslog alla versione r12.1 SP1 richiede l'aggiornamento delle integrazioni sugli agenti Windows (a pagina 70)

Capitolo 2: Ambiente operativo

Questa sezione contiene i seguenti argomenti:

Ambienti hardware e software

CA Enterprise Log Manager installa il sistema operativo Red Hat Enterprise Linux come parte dell'installazione iniziale.

L'indice della matrice di certificazione di CA Enterprise Log Manager elenca i collegamenti per tutte le matrici di certificazione di CA Enterprise Log Manager, inclusa la seguente:

- Hardware e software server

  Matrice di certificazione server hardware e software per CA Enterprise Log Manager

- Hardware e software agente

  Matrice di certificazione hardware e software dell'agente CA Enterprise Log Manager

- Sensori log e supporto del relativo sistema operativo

  Matrice di certificazione del sensore log di CA Enterprise Log Manager

- Integrazioni prodotto

  Matrice di integrazione del prodotto CA Enterprise Log Manager

- Certificazioni con CA Audit iRecorder

  Matrice di certificazione Audit iRecorder di CA Enterpise Log Manager

È possibile accedere a CA Enterprise Log Manager con i browser seguenti e il player Adobe Flash 9 o 10:

- Internet Explorer 6 SP2 (solo modalità Non FIPS)
- Internet Explorer 7 o 8 (modalità FIPS o Non FIPS)
- Mozilla Firefox 2.0.x e 3.0.x (solo modalità Non FIPS)
- Mozilla Firefox 3.5.8 o versioni successive (modalità FIPS e Non FIPS)

Nota: l'esportazione di file non è disponibile quando si accede a CA Enterprise Log Manager con un browser Mozilla Firefox.

Prerequisiti per le impostazioni di risparmio energetico per determinati tipi di computer HP e IBM

Quando CA Enterprise Log Manager viene installato su Server series HP Proliant DL 380G5 e IBM X3650 con le impostazioni predefinite di uso energetico, potrebbero verificarsi problemi iGateway che determinano un rallentamento del funzionamento oppure problemi di interfaccia che potrebbero richiedere un riavvio manuale del servizio.

Per impedire che questo problema potenziale si verifichi, modificare le impostazioni prima di installare CA Enterprise Log Manager:

Nota se CA Enterprise Log Manager è già stato installato, è possibile interrompere il computer, modificare le impostazioni secondo quanto indicato e riavviare il computer.

Per modificare le impostazioni di utilizzo energetico su HP Proliant DL 380G5

1. Accedere al menu BIOS Settings (Impostazioni di BIOS).
2. Accedere alle impostazioni di utilizzo energetico.
3. Selezionare OS Control Mode.

   Nota: l'impostazione predefinita corrisponde a HP Dynamic Power Settings Mode.

Per modificare le impostazioni di utilizzo energetico su IBM X3650

1. Accedere al menu BIOS Settings (Impostazioni di BIOS).
2. Accedere alle impostazioni di utilizzo energetico.
3. Disattivare i seguenti parametri:
   - Active Energy Manager
   - Enhanced C1 Power State

Risoluzione del monitor

Il requisito minimo di risoluzione del monitor è 1024 x 768 pixel. Per una visualizzazione ottimale, si consiglia una risoluzione del monitor di 1280 x 1024.

Riferimenti per il server CA EEM

Per informazioni sul supporto di sistemi operativi per un server CA EEM esistente, consultare la *Guida introduttiva a CA Embedded Entitlements Manager*. Questa guida è inclusa nel bookshelf di CA Enterprise Log Manager.

È anche possibile scaricare questo bookshelf dal Supporto tecnico. Per ottenere assistenza, contattare il supporto tecnico all'indirizzo http://ca.com/worldwide.

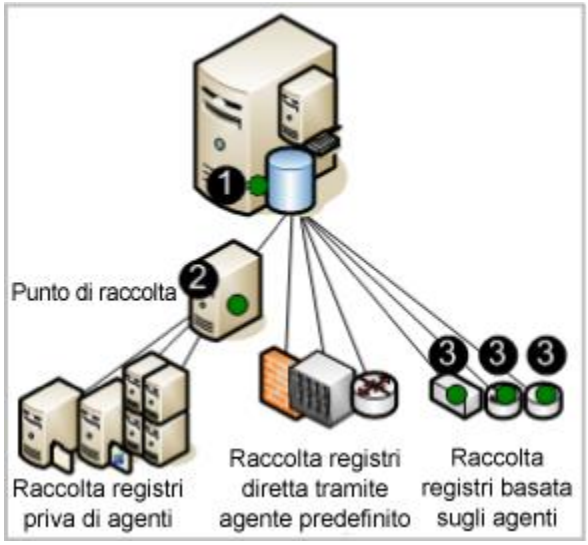
Capitolo 3: Funzioni

Questa sezione contiene i seguenti argomenti:

Raccolta registri

Il server CA Enterprise Log Manager può essere configurato per raccogliere i registri utilizzando una o più tecniche supportate. Le tecniche si differenziano per tipo e posizione del componente che ascolta e raccoglie i registri. Questi componenti sono configurati sugli agenti.

La seguente illustrazione raffigura un sistema a server singolo, in cui le posizioni dell'agente sono indicate con un cerchio scuro (verde).



I numeri sull'illustrazione fanno riferimento a questi passaggi:

1. Configurare l'agente predefinito su CA Enterprise Log Manager per recuperare gli eventi direttamente dalle origini syslog specificate.
2. Configurare l'agente installato su un punto di raccolta Windows per raccogliere gli eventi dai server Windows specificati e trasmetterli a CA Enterprise Log Manager.
3. Configurare gli agenti installati sugli host in cui le origini degli eventi sono in esecuzione per raccogliere il tipo di eventi configurato ed eseguire la soppressione.

Nota: il traffico dall'agente al server CA Enterprise Log Manager di destinazione è sempre crittografato.

Ciascuna tecnica di raccolta dei registri offre i seguenti vantaggi:

- Raccolta registri diretta

  Con la raccolta registri diretta, si configura il listener di syslog sull'agente predefinito per ricevere gli eventi dalle origini sicure specificate. È inoltre possibile configurare altri connettori per la raccolta degli eventi da qualsiasi origine di eventi compatibile con l'ambiente operativo del dispositivo software.

  Vantaggio: non è necessario installare un agente per raccogliere i registri dalle origini di eventi in prossimità del server CA Enterprise Log Manager.

- Raccolta senza agenti

  Con la raccolta senza agenti, non sono presenti agenti locali sulle origini degli eventi. Al contrario, un agente è installato su un punto di raccolta dedicato. Su tale agente sono configurati i connettori di ogni origine di evento di destinazione.

  Vantaggio: è possibile raccogliere i registri dalle origini degli eventi in esecuzione sui server dove non è possibile installare gli agenti, come i server in cui le regole aziendali proibiscono l'uso di agenti. L'invio è garantito, ad esempio, quando la raccolta dei registi ODBC è configurata correttamente.

- Raccolta basata su agenti

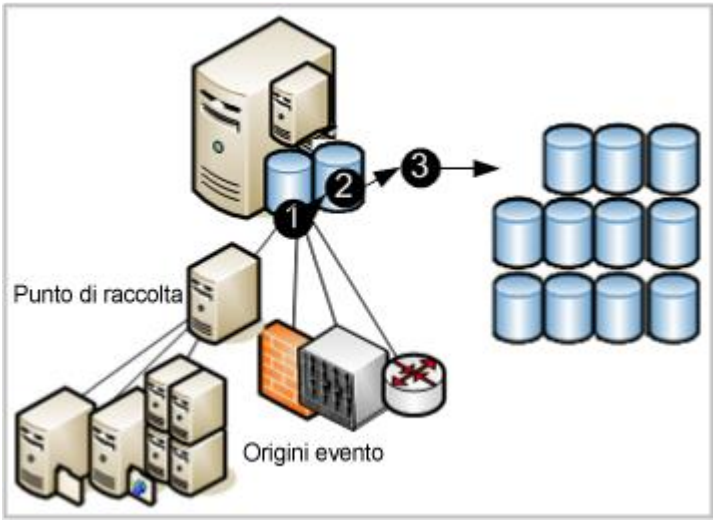
  Con la raccolta basata su agenti, viene installato un agente dove una o più origini di eventi sono in esecuzione ed è configurato un connettore per ogni origine di evento.

  Vantaggio: è possibile raccogliere i registri da un'origine dove la larghezza di banda della rete tra l'origine e CA Enterprise Log Manager non è sufficiente a supportare la raccolta dei registri diretta. È possibile utilizzare un agente per filtrare gli eventi e ridurre il traffico inviato nella rete. L'invio degli eventi è garantito.

Nota: consultare la *Guida all'amministrazione* per i dettagli sulla configurazione degli agenti.

Archiviazione dei registri

CA Enterprise Log Manager fornisce l'archiviazione dei registri incorporata gestita per i database archiviati di recente. Gli eventi raccolti dagli agenti dalle origini di eventi passano attraverso il ciclo di vita di archiviazione illustrato dal seguente schema.



I numeri sull'illustrazione fanno riferimento a questi passaggi:

1. I nuovi eventi raccolti tramite qualsiasi tecnica vengono inviati a CA Enterprise Log Manager. Lo stato degli eventi in entrata dipende dalla tecnica utilizzata per raccoglierli. Gli eventi in entrata devono essere perfezionati prima di essere inseriti nel database.
2. Quando il database dei record perfezionati raggiunge le dimensioni configurate, tutti i record vengono compressi in un database e salvati con un nome univoco. La compressione dei dati di registro ne riduce il costo di spostamento e archiviazione. Il database compresso può essere spostato automaticamente in base a una configurazione di autoarchiviazione oppure è possibile eseguirne il backup e spostarlo manualmente prima che raggiunga l'età configurata per l'eliminazione. I database autoarchiviati vengono eliminati dall'origine non appena vengono spostati.
3. Se si configura l'autoarchiviazione per spostare i database compressi in un server remoto su base giornaliera, è possibile spostare questi backup in un archivio off-site a lungo termine a propria discrezione. La conservazione dei backup dei registri permette di mantenere la conformità alle normative stando alle quali i registri devono essere raccolti in modo sicuro, archiviati centralmente per un certo numero di anni e disponibili per la consultazione. È possibile ripristinare il database dall'archivio a lungo termine in qualsiasi momento.

Nota: consultare la *Guida all'implementazione* per i dettagli sulla configurazione dell'archivio del registro eventi, inclusa la configurazione dell'autoarchiviazione. Consultare la *Guida all'amministrazione* per i dettagli sul ripristino dei backup per l'analisi e il reporting.

Presentazione standardizzata dei registri

I registri generati da applicazioni, sistemi operativi e periferiche utilizzano tutti il proprio formato. CA Enterprise Log Manager perfeziona i registri raccolti per standardizzare il metodo di rapporto dei dati. Il formato standard rende più semplice per i revisori e la direzione confrontare i dati raccolti da origini diverse. Tecnicamente, la Grammatica evento comune (CEG) di CA semplifica l'implementazione della normalizzazione e della classificazione degli eventi.

La CEG fornisce diversi campi utilizzati per normalizzare vari aspetti dell'evento, inclusi i seguenti:

- Modello ideale (classe di tecnologie come antivirus, DBMS e firewall)
- Categoria (alcuni esempi sono la Gestione identità e la Protezione di rete)
- Classe (alcuni esempi sono Gestione account e Gestione gruppo)
- Azione (alcuni esempi sono Creazione account e Creazione gruppo)
- Risultati (alcuni esempi sono Operazione riuscita e Operazione non riuscita)

Nota: consultare *Guida all'amministrazione di CA Enterprise Log Manager* per i dettagli sulle regole e i file utilizzati nel perfezionamento degli eventi. Per ulteriori informazioni sulla normalizzazione e sulla categorizzazione degli eventi, consultare la sezione della guida in linea dedicata alla Grammatica comune evento.

Creazione di rapporti di conformità

CA Enterprise Log Manager permette di raccogliere ed elaborare dati rilevanti per la sicurezza e trasformarli in rapporti adatti per revisori interni o esterni. È possibile interagire con query e rapporti per le analisi. È possibile automatizzare la procedura di creazione dei rapporti pianificando le operazioni relative ai rapporti.

Il sistema fornisce:

- Semplici funzionalità di query con tag
- Dati in tempo reale
- Archivi dei registri critici distribuiti a livello centrale e disponibili per la ricerca

Si concentra sui rapporti di conformità anziché sulla correlazione in tempo reale di eventi e avvisi. Le normative richiedono rapporti che dimostrano la conformità con i controlli di settore. CA Enterprise Log Manager fornisce rapporti con i seguenti tag per l'identificazione rapida:

- Basel II
- COBIT
- COSO
- Direttiva UE - Protezione dei dati
- FISMA
- GLBA
- HIPAA
- ISO\IEC 27001\2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS 70
- SOX

È possibile rivedere i rapporti dei registri predefiniti o eseguire ricerche in base ai criteri specificati. I nuovi rapporti sono forniti con gli aggiornamenti della sottoscrizione.

Le capacità di visualizzazione dei registri sono supportate da quanto segue:

- Funzione di query su richiesta con query predefinite o definite dall'utente, i cui risultati possono includere fino a 5000 record
- Ricerca rapida attraverso prompt di un nome host, indirizzo IP, numero di porta o nome utente specificato
- Rapporti pianificati e su richiesta con contenuto dei rapporti subito disponibile
- Query e avvisi pianificati
- Rapporti di base con informazioni sugli andamenti
- Visualizzatori eventi grafici e interattivi
- Creazione automatizzata di rapporti con allegati di posta elettronica
- Criteri di memorizzazione automatica dei rapporti

Nota: per i dettagli sull'utilizzo di query e rapporti predefiniti o sulla creazione di modelli personalizzati, consultare la *Guida all'amministrazione di CA Enterprise Log Manager*.

Avviso di violazione del criterio

CA Enterprise Log Manager permette di automatizzare l'invio di un avviso quando si verifica un evento che richiede attenzione a breve termine. È possibile anche monitorare gli avvisi di CA Enterprise Log Manager in ogni momento specificando un intervallo di tempo, dagli ultimi cinque minuti fino agli ultimi 30 giorni. Gli avvisi vengono inviati automaticamente a un feed RSS accessibile da qualsiasi browser Web. Facoltativamente, è possibile specificare altre destinazioni, inclusi indirizzi e-mail, una procedura di CA IT PAM come quella che genera i ticket dell'assistenza tecnica e uno o più indirizzi IP di destinazione dei trap SNMP.

Per aiutare l'utente, sono disponibili molte query predefinite da utilizzare così come sono per la pianificazione come avvisi. Gli esempi includono:

- Attività utente eccessiva
- Media di utilizzo della CPU alta
- Spazio su disco insufficiente
- Registro evento protezione eliminato nelle ultime 24 ore
- Criterio di controllo Windows modificato nelle ultime 24 ore

Alcune query utilizzano elenchi con chiave dove si forniscono i valori utilizzati nella query. Alcuni elenchi con chiave includono valori predefiniti ai quali è possibile aggiungerne altri. Gli esempi includono account predefiniti e gruppi con privilegi. Altri elenchi con chiave, come quello per le risorse aziendali critiche, non dispongono di valori predefiniti. Una volta configurati, gli avvisi possono essere pianificati per query predefinite come:

- Aggiunta o rimozione di appartenenza al gruppo attraverso gruppi con privilegi
- Accessi completati con successo da parte dell'account predefinito
- Nessun evento ricevuto dalle origini critiche di business

Gli elenchi con chiave possono essere aggiornati manualmente, importando un file o eseguendo una procedura CA IT PAM di valori dinamici.

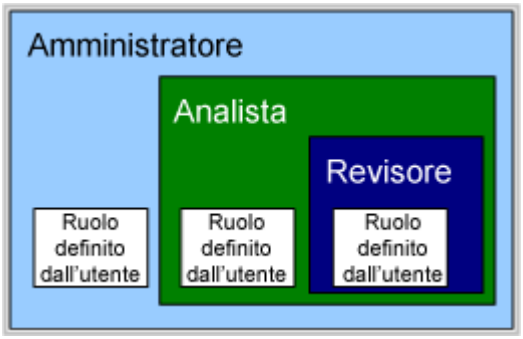
Nota: per i dettagli sugli avvisi consultare la *Guida all'amministrazione di CA Enterprise Log Manager*.

Accesso in base ai ruoli

CA Enterprise Log Manager fornisce tre ruoli o gruppi applicazioni predefiniti. Gli amministratori assegnano i seguenti ruoli agli utenti per specificarne i diritti di accesso alle funzioni di CA Enterprise Log Manager:

- Amministratore
- Analista
- Revisore

Il Revisore ha accesso alle nuove funzioni. L'Analista ha accesso a tutti le funzioni del Revisore e ad alcune altre. L'Amministratore ha accesso a tutte le funzioni. È possibile definire un ruolo personalizzato con criteri associati che limitano l'accesso dell'utente alle risorse, secondo le esigenze aziendali.



Gli amministratori possono personalizzare l'accesso a qualsiasi risorsa creando un gruppo applicazioni personalizzato con criteri associati e assegnando tale gruppo applicazioni, o ruolo , agli account utente.

Nota: consultare la *Guida all'amministrazione CA Enterprise Log Manager* per dettagli sulla pianificazione e la creazione di ruoli predefiniti, criteri predefiniti e filtri di accesso.

Gestione sottoscrizioni

Un modulo di sottoscrizione è un servizio che consente di scaricare automaticamente gli aggiornamenti di sottoscrizione dal server di sottoscrizione CA in base ad una pianificazione e di distribuirli a tutti i server CA Enterprise Log Manager. Quando un aggiornamento di sottoscrizione include il modulo per gli agenti, gli utenti avviano la distribuzione di questi aggiornamenti negli agenti. *Gli aggiornamenti di sottoscrizione* sono aggiornamenti ai componenti software CA Enterprise Log Manager, aggiornamenti e patch del sistema operativo e aggiornamenti di contenuti quali i rapporti.

La seguente illustrazione raffigura lo scenario più semplice di connessione diretta ad Internet:

I numeri sull'illustrazione fanno riferimento a questi passaggi:

1. Come server di sottoscrizione predefinito, il server CA Enterprise Log Manager contatta il server di sottoscrizione CA per gli aggiornamenti e scarica tutti i nuovi aggiornamenti disponibili. Il server CA Enterprise Log Manager crea un backup, quindi invia gli aggiornamenti di contenuto al componente integrato del server di gestione che archivia gli aggiornamenti di contenuto per tutti gli altri CA Enterprise Log Manager.
2. Come client di sottoscrizione, il server CA Enterprise Log Manager auto-installa gli aggiornamenti del prodotto e del sistema operativo necessari.

Nota: consultare la *Guida all'implementazione* per i dettagli sulla pianificazione e la configurazione della sottoscrizione. Consultare la *Guida all'amministrazione* per i dettagli sul perfezionamento e la modifica della configurazione della sottoscrizione e per applicare gli aggiornamenti agli agenti.

Supporto per indirizzi IP IPv6

In precedenza, la specifica degli indirizzi IP era limitata alla notazione decimale separata da punti IPv4. La versione corrente consente di specificare indirizzi IPv6 in qualunque campo per indirizzo IP. IPv6 utilizza indirizzi IP a 128 bit invece di quelli a 32 bit utilizzati da IPv4. Qualunque criterio basato sulla versione dell'indirizzo IP supporta sia IPv6 che IPv4.

È possibile utilizzare indirizzi IPv6 con mapping IPv4 o il formato IPv6 tradizionale. Il formato dell'indirizzo IPv6 con mapping IPv4 permette di rappresentare l'indirizzo IPv4 di un nodo IPv4 come indirizzo IPv6, come descritto di seguito:

- Il formato preferito IPv6 è formato da otto gruppi di quattro cifre esadecimali (x:x:x:x:x:x:x:x). Ogni x rappresenta da una a quattro cifre esadecimali delle otto parti a 16 bit dell'indirizzo.
- L'indirizzo IPv6 con mapping IPv4, pratico in un ambiente misto di nodi IPv4 e IPv6, è 0:0:0:0:0:FFFF:d.d.d.d, dove ogni d rappresenta uno dei valori decimali dell'indirizzo (notazione decimale separata da punti IPv4).

  Importante: gli indirizzi IPv6 compatibili con IPv4 nel formato 0:0:0:0:0:0:d.d.d.d sono ormai obsoleti, in base alla RFC 4291, perché gli attuali meccanismi di transizione a IPv6 non utilizzano più questi indirizzi.

Quello che segue è un indirizzo IPv6 valido scritto nel formato tradizionale.

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Se uno o più gruppi di quattro cifre è 0000, è possibile omettere gli zeri e sostituirli con due segni di due punti (::). È possibile omettere anche gli zeri iniziali di un gruppo. Gli indirizzi IP di esempio che seguono sono equivalenti:

- 2001:0db8:0000:0000:0000:0000:1428:57ab
- 2001:0db8::1428:57ab
- 2001:db8:0:0:0:0:1428:57ab
- 2001:db8::1428:57ab

Per sostituire gli indirizzi IPv4 con degli indirizzi con mapping IPv4, utilizzare gli esempi seguenti come indicazioni:

- 0:0:0:0:0:FFFF:192.168.2.128
- 0:0:0:0:0:FFFF:172.16.2.128

In alternativa, è possibile utilizzare la forma compressa seguente:

- ::FFFF:192.168.2.128
- ::FFFF:172.16.2.128

Capitolo 4: Funzionalità nuove ed aggiornate nella versione r12.1

Questa sezione contiene i seguenti argomenti:

Accesso Open API

CA Enterprise Log Manager permette di utilizzare le chiamate API per accedere ai dati dal repository di eventi utilizzando il meccanismo di query e rapporti e di visualizzare i dati in un browser Web. È inoltre possibile utilizzare l'API per incorporare le query o i rapporti CA Enterprise Log Manager nell'interfaccia di un prodotto CA o di terze parti.

Le funzionalità delle API CA Enterprise Log Manager comprendono:

- API sicure e autenticate
- Registrazione del prodotto per Single Sign-On (SSO)
- Recupero di un elenco di query o rapporti, filtrato per tag
- Visualizzazione di query o rapporti nell'interfaccia CA Enterprise Log Manager interattiva, con funzioni di filtraggio e integrazione in un'interfaccia utente

Ulteriori informazioni sulle API sono disponibili nella *Guida di programmazione API* e nella Guida in linea.

Avvisi attivabili: integrazione di CA IT PAM

Attraverso avvisi pianificati che interrogano i volumi dei record di registro, CA Enterprise Log Manager rileva potenziali violazioni del controllo e attività IT sospette. CA Enterprise Log Manager invia la notifica allo staff della sicurezza IT che analizza ogni avviso per determinare le azioni correttive necessarie. Le attività di analisi tipiche sono spesso di routine e adatte all'automazione. Attraverso una stretta integrazione tra CA Enterprise Log Manager e CA IT PAM, queste azioni di risposta di routine possono essere eseguite automaticamente. Lo staff della sicurezza IT è svincolato da attività ripetitive e può concentrarsi solo sulle questioni più importanti.

L'integrazione di CA IT PAM permette di creare richieste in CA Service Desk eseguendo dagli avvisi un processo CA IT PAM di output di evento/avviso predefinito. È inoltre possibile eseguire processi IT PAM di output di evento/avviso da CA Enterprise Log Manager per automatizzare altre risposte rispetto a eventi sospetti.

Per ulteriori dettagli, consultare la sezione "Operazioni con processi CA IT PAM di evento/avviso" nel capitolo Avvisi della *Guida all'amministrazione* di CA Enterprise Log Manager.

Avvisi attivabili: integrazione SNMP con prodotti NSM

Gli avvisi sono generati quando le query pianificate recuperano eventi che indicano attività sospette. È possibile automatizzare l'invio di avvisi come trap SNMP per prodotti di monitoraggio della sicurezza di rete (NSM) come CA Spectrum o CA NSM. Preparare i prodotti di destinazione per la ricezione e l'interpretazione di trap SNMP da CA Enterprise Log Manager, configurare i percorsi di destinazione, quindi specificare le informazioni dell'evento da inviare.

Per ulteriori dettagli, consultare la sezione "Operazioni con trap SNMP" nel capitolo Avvisi della *Guida all'amministrazione* di CA Enterprise Log Manager.

Accesso ODBC e JDBC

CA Enterprise Log Manager permette l'accesso in sola lettura alle informazioni del registro eventi raccolte utilizzando ODBC e JDBC. È possibile utilizzare questo accesso per eseguire operazioni come le seguenti:

- Creare rapporti personalizzati utilizzando strumenti come BusinessObjects Crystal Reports

- Recuperare informazioni dei registri selezionati per l'utilizzo con un motore di correlazione
- Esaminare i registri per il rilevamento di intrusioni o malware

Le funzionalità di accesso ODBC e JDBC utilizzano un client da installare su un determinato server in rete. Il server CA Enterprise Log Manager installa automaticamente i propri componenti lato server durante l'aggiornamento della sottoscrizione e l'elaborazione dell'installazione.

Informazioni sull'installazione sono disponibili nella *Guida all'implementazione*. Informazioni ed esempi sulla configurazione sono disponibili nella *Guida all'amministrazione*.

Rilevanza identità e asset: integrazione di CA IT PAM

L'integrazione di CA IT PAM permette di conservare i valori degli aggiornamenti per una determinata chiave eseguendo una procedura di valori dinamici di CA IT PAM. Una procedura di valori dinamici recupera i valori correnti dai repository che archiviano i dati correnti. Se si crea una procedura che recupera i valori degli asset fondamentali dal file o dal database degli asset, è possibile aggiornare la chiave Critical_Assets nei rapporti e nelle query predefinite con un solo clic.

Per ulteriori dettagli, consultare la sezione "Abilitare l'importazione di valori dinamici" nel capitolo Query e rapporti della *Guida all'amministrazione* di CA Enterprise Log Manager.

Raccolta diretta di registri estesa da parte dell'agente predefinito

All'installazione di CA Enterprise Log Manager, il listener di syslog, chiamato Syslog_Connector, viene distribuito sull'agente predefinito per abilitare la raccolta degli eventi di syslog. Anche l'integrazione Linux_localsyslog, con il connettore associato Linux_localsyslog_Connector, è disponibile per la raccolta di eventi syslog.

L'agente predefinito ora può raccogliere in modo diretto non solo gli eventi syslog. Utilizzando il connettore WinRm, l'agente predefinito può raccogliere eventi da prodotti in esecuzione su piattaforme Microsoft Windows, come Servizi certificati Active Directory e Microsoft Office Communication Server. Utilizzando il connettore ODBC, l'agente predefinito può raccogliere eventi da diversi database come Oracle9i e SQL Server 2005 e applicazioni che archiviano i propri eventi in questi database.

Pianificazione di aggiornamento automatizzata per i client di sottoscrizione

Installando il primo server CA Enterprise Log Manager, configurare le impostazioni globali di tutti i servizi, compresa la sottoscrizione. Per motivi di sottoscrizione, il primo server installato è il proxy di sottoscrizione predefinito. Configurare l'ora di avvio dell'aggiornamento e la frequenza con cui il proxy controlla gli aggiornamenti nel server di sottoscrizione di CA. Installando server aggiuntivi, per impostazione predefinita verranno installati come client di sottoscrizione. Configurare i server aggiuntivi a livello locale. La configurazione a livello locale viene eseguita selezionando il nome del server da configurare ed ignorando le configurazioni globali selezionate.

Per impostazione predefinita, l'ora di inizio dell'aggiornamento dei client di sottoscrizione viene ereditata dalle impostazioni globali. Possono verificarsi problemi quando le impostazioni ereditate non vengono annullate manualmente per forzare un ritardo. Per prevenire questo problema, la pianificazione di aggiornamento per i client viene adesso automatizzata con un ritardo di 15 minuti. Non bisogna più configurare manualmente la pianificazione di aggiornamento per i client di sottoscrizione.

Capitolo 5: Funzionalità nuove e modificate nella versione r12.1 SP1

Questa sezione contiene i seguenti argomenti:

Panoramica della conformità FIPS 140-2

Il Federal Information Processing Standard (FIPS) 140-2 è uno standard di sicurezza per le librerie di crittografia e gli algoritmi da utilizzare per la crittografia. La crittografia FIPS 140-2 interessa la trasmissione dei dati sensibili tra i componenti dei prodotti CA e tra prodotti CA e prodotti di terze parti. Lo standard FIPS 140-2 specifica i requisiti per l'utilizzo di algoritmi di crittografia in un sistema di sicurezza per la protezione di dati sensibili non classificati.

CA Enterprise Log Manager offre la compatibilità con FIPS per il traffico degli eventi protetti mediante algoritmi conformi con gli standard FIPS durante operazioni in modalità FIPS. Inoltre, è disponibile una modalità Non FIPS predefinita, in cui il traffico eventi *non* viene protetto con algoritmi FIPS. I server CA Enterprise Log Manager in una rete federata non possono combinare le due modalità operative. Ciò significa che un server in esecuzione in modalità Non FIPS non può condividere query e dati di rapporto con un server in esecuzione in modalità FIPS.

Per informazioni sull'attivazione e la disattivazione della modalità FIPS, consultare la sezione sull'installazione di CA Enterprise Log Manager della *Guida all'implementazione* oppure la Guida in linea del servizio Stato del sistema.

Ulteriori informazioni:

Modalità operative

CA Enterprise Log Manager può operare in due modalità: FIPS o Non FIPS. I limiti di crittografia sono gli stessi in entrambe le modalità, ma gli algoritmi sono differenti. Per impostazione predefinita, i server CA Enterprise Log Manager operano in modalità Non FIPS. Gli utenti con ruolo di amministratore possono attivare la modalità operativa FIPS.

Modalità Non FIPS

Questa modalità utilizza un insieme di algoritmi di crittografia per il trasporto eventi e altre comunicazioni tra il server CA Enterprise Log Manager e il server CA EEM che non soddisfano necessariamente gli standard FIPS 140-2.

Modalità FIPS

Questa modalità utilizza algoritmi di crittografia FIPS per il trasporto eventi e altre comunicazioni tra il server CA Enterprise Log Manager e il server CA EEM.

Gli utenti con diritti di amministrazione possono controllare le modalità operative dell'agente dal nodo Gestione agenti nella scheda secondaria Raccolta log della scheda Amministrazione.

Per ulteriori informazioni sul passaggio dalla modalità FIPS alla modalità Non FIPS, consultare la Guida in linea delle Attività di stato del sistema oppure la sezione relativa alla configurazione dei servizi della *Guida all'implementazione*.

Librerie di crittografia

La pubblicazione sul Federal information Processing Standard (FIPS) 140-2 specifica i requisiti per l'utilizzo di algoritmi di crittografia in un sistema di sicurezza per la protezione di dati sensibili non classificati.

CA Enterprise Log Manager incorpora la libreria di crittografia RSA Crypto-C Micro Edition (ME) v2.1.0.2, ritenuta conforme ai requisiti FIPS 140-2 per la *sicurezza dei moduli crittografici (Security Requirements for Cryptographic Modules).* Il numero del certificato di convalida per questo modulo è 865.

Algoritmi utilizzati

Computer che utilizzano moduli crittografici certificati FIPS 140-2 in modalità FIPS possono utilizzare solo funzioni di protezione FIPS, quali AES (Advanced Encryption Algorithm), SHA-1 (Secure Hash Algorithm) e protocolli di livello superiore, quali TLS v1.0 come esplicitamente consentito negli standard FIPS 140-2 e nelle guide all'implementazione.

In modalità Non FIPS, CA Enterprise Log Manager utilizza i seguenti algoritmi:

- AES 128
- Triple DES (3DES)
- SHA-1
- MD5
- SSL V3

In modalità FIPS, CA Enterprise Log Manager utilizza i seguenti algoritmi:

- AES 128
- Triple DES (3DES)
- SHA-1
- TLS V1

CA Enterprise Log Manager utilizza SHA-1 come algoritmo digest predefinito per crittografare le password e firmare le richieste al server.

CA Enterprise Log Manager utilizza TLS v1.0 per comunicazioni con directory LDAP esterne se la connessione LDAP utilizza TLS, comunicazioni tra componenti iTechnology, agenti di comunicazione con il servizio iGateway in modalità FIPS e canali di eventi tra un agente e il servizio logDepot.

Informazioni sui certificati e i file di chiave

Per il supporto FIPS 140-2, l' aggiornamento a CA Enterprise Log Manager r12.1 SP1 converte i certificati esistenti in formato P12 in certificati in formato PEM. La conversione determina la creazione dei seguenti file:

- File di certificato con estensione .cer
- File di chiave con estensione .key

I file di chiave non sono crittografati, per cui sarà responsabilità dell'utente proteggerli dall'accesso non autorizzato sugli host del server e dell'agente. Il dispositivo software CA Enterprise Log Manager utilizza varie tecniche di protezione avanzata del sistema operativo per proteggere le chiavi e certificati archiviati nel file system. CA Enterprise Log Manager non supporta l'utilizzo di dispositivi di archiviazione di chiave esterni.

CA Enterprise Log Manager utilizza i seguenti certificati e file di chiave:

Nome file del certificato/della chiave	Posizione	Descrizione
CAELMCert	/opt/CA/SharedComponents/iTechnology (È possibile fare riferimento a questa directory utilizzando il nome breve della variabile, $IGW _ LOC.)	Tutti i servizi CA Enterprise Log Manager utilizzano questo certificato per le comunicazioni tra i server CA Enterprise Log Manager e tra i server CA Enterprise Log Manager e il server CA EEM. Nel file di configurazione principale CALM.cnf, è presente una voce per il certificato e il relativo file di chiave. La coppia di tag inizia rispettivamente per <Certificate> e <KeyFile>.
CAELM_AgentCert	$IGW _ LoC sul server host agente	Gli agenti utilizzano questo certificato per comunicare con i server CA Enterprise Log Manager. Il server di gestione CA Enterprise Log Manager fornisce il certificato all'agente. Il certificato è valido per tutti i server CA Enterprise Log Manager all'interno di una determinata istanza di applicazione.
itpamcert	Server IT PAM	Questo certificato viene utilizzato per la comunicazione con IT PAM. Per ulteriori informazioni, consultare la documentazione di CA IT PAM.

Nome file del certificato/della chiave	Posizione	Descrizione
rootcert	$IGW_LOC	Questo certificato è un certificato root autofirmato da iGateway durante l'installazione.
iPozDsa	$IGW_LOC	Questo certificato è utilizzato dal server CA EEM, locale e remoto. Per ulteriori informazioni, consultare la documentazione di CA EEM.
iPozRouterDsa	$IGW_LOC	Questo certificato è utilizzato dal server CA EEM, locale e remoto. Per ulteriori informazioni, consultare la documentazione di CA EEM.
iTechPoz-trusted	/opt/CA/Directory/dxserver/.config/ssld	Questo certificato è utilizzato da CA Directory.
iTechPoz-<hostname>-Router	/opt/CA/Directory/dxserver/.config/ssld	Questo certificato è utilizzato da CA Directory.

Limitazioni del supporto FIPS

Le seguenti funzionalità di CA Enterprise Log Manager e interoperabilità di prodotto non supportano operazioni in modalità FIPS:

Accesso ODBC e JDBC al deposito eventi di log

In CA Enterprise Log Manager, l'accesso ODBC e JDBC si basa su un SDK che non supporta modalità operative FIPS. Gli amministratori di reti federate che richiedono operazioni FIPS devono disabilitare manualmente il servizio ODBC su tutti i server CA Enterprise Log Manager. Consultare la sezione relativa alla disabilitazione dell'accesso ODBC e JDBC al deposito eventi di log della *Guida all'implementazione*.

Condivisione di un server CA EEM

CA Enterprise Log Manager r12.1 SP1 utilizza CA EEM r8.4 SP3, compatibile con FIPS. L'abilitazione della modalità FIPS sul server CA Enterprise Log Manager disabilita la comunicazione tra il server CA EEM condiviso e qualsiasi prodotto che non supporta CA EEM r8.4 SP3.

Ad esempio, CA IT PAM non è compatibile con FIPS. Se si esegue l'aggiornamento del server CA Enterprise Log Manager in modalità FIPS, l'integrazione con CA IT PAM non verrà eseguita.

È possibile eseguire la condivisione di un server CA EEM tra CA Enterprise Log Manager r12.1 SP1 e CA IT PAM r2.1 SP2 e r2.1 SP3 solo in modalità Non FIPS.

Se l' installazione di CA IT PAM dell'utente non condivide lo stesso server di CA EEM, CA Enterprise Log Manager r12.1 SP1 potrà essere eseguito in modalità FIPS e comunicare con CA IT PAM ma tali canali di comunicazione non saranno compatibili con FIPS.

Corrispondenza di modalità operative per le operazioni di binding

La corretta comunicazione con un archivio utenti esterno dipende da quanto segue:

- I server CA Enterprise Log Manager e il loro server di gestione CA EEM devono essere nella stessa modalità FIPS.
- Il server CA EEM deve essere nella stessa modalità FIPS dell'archivio utenti esterno abilitato per FIPS quando si utilizza TLS v 1.0 per la connessione.

  Nota: la compatibilità con FIPS non è disponibile quando si utilizzano comunicazioni non crittografate tra il server CA EEM e l'archivio utenti esterno oppure quando il server CA EEM e l'archivio utenti presentano modalità FIPS differenti.

Trap SNMP

È possibile inviare eventi SNMP utilizzando SNMP V2 o SNMP V3. Entrambi i protocolli sono supportati in modalità Non FIPS.

Se il server di destinazione dei trap SNMP è abilitato per FIPS, è necessario optare per la Protezione V3, quindi scegliere SHA come protocollo di autenticazione e AES come protocollo di crittografia. Effettuare le proprie selezioni nella pagina Destinazione della procedura guidata di pianificazione avvisi.

Configurazione di Microsoft Internet Explorer per l'accesso a CA Enterprise Log Manager in modalità FIPS

Per poter visualizzare l'interfaccia utente del server CA Enterprise Log Manager, il browser in uso potrebbe richiedere ulteriori configurazioni se è in esecuzione in modalità FIPS. Per impostare le opzioni di accesso a CA Enterprise Log Manager in Microsoft Internet Explorer 7 o 8, utilizzare la procedura riportata a continuazione.

Nota: non è possibile utilizzare Microsoft Internet Explorer 6 per accedere a server CA Enterprise Log Manager in esecuzione in modalità FIPS.

Per configurare Microsoft Internet Explorer 7 o 8:

1. Aprire il browser e selezionare Strumenti, Opzioni Internet.
2. Selezionare la scheda Avanzate e scorrere fino alla sezione Protezione.
3. Selezionare tutte le seguenti opzioni:
   - Usa SSL 2.0
   - Usa SSL 3.0
   - Usa TLS 1.0
4. Fare clic su OK.

Configurazione di Mozilla Firefox per l'accesso a CA Enterprise Log Manager in modalità FIPS

Per poter visualizzare l'interfaccia utente del server CA Enterprise Log Manager, il browser in uso potrebbe richiedere ulteriori configurazioni se è in esecuzione in modalità FIPS. Utilizzare la seguente procedura per impostare le opzioni necessarie in Mozilla Firefox 3.5.8 o versioni successive del browser per accedere a un server CA Enterprise Log Manager in esecuzione in modalità FIPS.

Nota: l'accesso a CA Enterprise Log Manager richiede l'installazione del plugin di Mozilla Firefox per Adobe Flash 9 o 10.

Per configurare Mozilla Firefox:

1. Aprire il browser e selezionare Strumenti, Opzioni.
2. Fare clic sulla scheda Avanzate, quindi sulla scheda secondaria Crittografia.
3. Selezionare entrambe le seguenti opzioni:
   - Usa SSL 3.0
   - Usa TLS 1.0
4. Selezionare la scheda secondaria Protezione, quindi l'opzione per l' utilizzo di una password master.
5. Fare clic su Cambia password master... e fornire una password adeguata all'apertura della finestra, quindi fare clic su OK.
6. Selezionare la scheda secondaria Avanzate.
7. Fare clic su Dispositivi di sicurezza.

   Viene visualizzata la finestra Dispositivi di sicurezza.
8. Selezionare il modulo NSS interno PKCS# 11 nel riquadro sinistro.

   In tal modo verrà compilato automaticamente il riquadro destro.
9. Selezionare la riga Module NSS Internal FIPS PKCS #11 Module e fare clic sull'opzione di abilitazione FIPS.
10. Quando richiesto, immettere la password master creata precedentemente, quindi fare clic su OK.
11. Fare clic su OK nella finestra Gestione periferiche.
12. Fare clic su OK nella finestra Opzioni.
13. Riavviare il browser.

Ulteriori informazioni:

Aggiornamento attraverso sottoscrizione (a pagina 11)

Immagine ISO per nuove installazioni

Un'immagine ISO fornita con il Service Pack aiuta l'utente a distribuire velocemente CA Enterprise Log Manager o ad aggiungere un nuovo server CA Enterprise Log Manager a una distribuzione esistente. L'immagine ISO è disponibile nell'area di download del supporto tecnico in linea.

Si consiglia l'utilizzo dell'immagine ISO più recente per i seguenti casi:

- Distribuzione di CA Enterprise Log Manager. L'installazione dell'immagine ISO più recente riduce il numero di aggiornamenti della sottoscrizione da applicare e rende più veloce la distribuzione.
- Aggiunta di un nuovo server CA Enterprise Log Manager dopo aver aggiornato i server nella distribuzione esistente. In primo luogo verificare che i server e gli agenti della distribuzione corrente siano stati aggiornati correttamente ed abilitati a ricevere eventi. Quindi installare i nuovi server mediante l'immagine ISO per aggiungere ulteriore capacità e ridurre il numero di aggiornamenti della sottoscrizione da applicare.

Nota: la procedura di installazione è stata modificata. Un nuovo prompt richiede se si desidera eseguire l'installazione con la modalità FIPS abilitata. Quando si aggiunge un nuovo server CA Enterprise Log Manager ad una distribuzione FIPS esistente, è necessario abilitare la modalità FIPS durante l'installazione (il server di gestione CA Enterprise Log Manager o il server CA EEM remoto sono in modalità FIPS). Se la modalità FIPS non viene abilitata, il nuovo server non potrà essere registrato e sarà necessario reinstallarlo. Per ulteriori informazioni sulla modalità FIPS, consultare la *Guida all'implementazione*.

Capitolo 6: Problemi noti

Questa sezione contiene i seguenti argomenti:

Agenti e adapter CA

Quelli descritti di seguito sono i problemi noti relativi agli agenti e agli adapter CA.

Dipendenza dell'installazione dell'agente su Red Hat Linux 4

Sintomo:

Quando si installa l'agente CA Enterprise Log Manager su sistemi Red Hat Enterprise Linux 4, l'installazione non riesce e visualizza un messaggio di errore relativo alle dipendenze richieste.

Soluzione:

L'agente CA Enterprise Log Manager su Red Hat Enterprise Linux 4 richiede il pacchetto Legacy Software Development. Installare il pacchetto di sviluppo software legacy prima di installare l'agente.

Accuratezza dell'ora di stato agente basata sulla configurazione del server NTP

Sintomo:

Se più server CA Enterprise Log Manager che eseguono la raccolta sono impostati manualmente su diversi orologi, può verificarsi una discrepanza in merito al tempo di attività segnalato per l'agente.

Soluzione:

Quando si installano server CA Enterprise Log Manager nella rete, specificare un server NTP. Configurare server NTP per ciascun server sincronizza l'ora riportata per gli agenti gestiti da server diversi.

Considerare il tempo necessario per eseguire l'aggiornamento dopo aver eseguito la distribuzione connettori in blocco

Sintomo:

Dopo aver eseguito la Distribuzione connettori in blocco, i nuovi connettori non vengono immediatamente visualizzati nell'Explorer agente.

Soluzione:

In base al numero di connettori e degli agenti sui quali verranno distribuiti, attendere alcuni minuti prima di aggiornare tutti i connettori nell'Explorer agente.

Distribuzione connettori in blocco con indirizzo IPv6 non eseguita correttamente

Sintomo:

La distribuzione dei connettori tramite la procedura guidata di Distribuzione connettori in blocco fornisce un indirizzo server in formato IPV6, impedendone il funzionamento previsto. Dopo alcuni istanti, lo stato del connettore verrà visualizzato come In esecuzione. Quando si modifica il connettore, si può notare che il nome server visualizza nell'indirizzo IPV6 soltanto le prime quattro cifre. Il nome utente, la password e i campi di dominio risulteranno vuoti.

Soluzione:

Attualmente, l'interfaccia utente CA Enterprise Log Manager invia i contenuti del file di origine utilizzando :: come delimitatore per separare ciascuna origine. Poiché l'indirizzo IPv6 contiene i due punti riportati per due volte consecutive (::), esso viene elaborato come un delimitatore. Il record del connettore non è stato salvato correttamente.

Non utilizzare indirizzi IPv6 per eseguire la distribuzione dei connettori in blocco. Per configurare i connettori per la distribuzione in blocco, è *possibile* utilizzare nomi host. È inoltre possibile configurare un connettore IPv6 dalla procedura guidata di Creazione nuovo connettore, utilizzando le istruzioni standard.

Il nome di montaggio del DVD non può contenere spazi

Sintomo:

Quando si installa manualmente un agente dal DVD-ROM del prodotto su un computer con sistema operativo Linux, viene visualizzato un messaggio di errore di autorizzazione negata e l'installazione si chiude.

Soluzione:

Per installare un agente dal supporto DVD, è necessario montare l'unità DVD con un comando simile al seguente:

```
$ mount /dev/cdrom <percorso locale>
```

Il DVD-ROM non può essere montato su un nome di percorso locale (directory) che contenga spazi. Montare il DVD-ROM su un nome di directory che non contenga spazi, quindi installare l'agente.

La configurazione dell'origine evento di livello di dominio non è riuscita

Sintomo:

Per configurare un qualsiasi connettore per accedere a un'origine eventi Windows e leggere i relativi registri occorre creare un account utente a bassi privilegi ed assegnare ad esso le autorizzazioni necessarie. Se l'origine evento è un host Windows Server 2003 SP1, uno dei passaggi consiste nell'impostare il criterio di protezione locale *Impersonare un client dopo l'autenticazione*. Quando il diritto utente viene impostato localmente, non si verifica alcun inconveniente. Tuttavia, se questa impostazione viene applicata a tutti i server come criterio di dominio, l'applicazione globale eliminerà le assegnazioni locali esistenti per gli altri utenti, ovvero Amministratori e SERVIZIO.

Secondo un articolo del supporto tecnico Microsoft, "si verificano problemi collegando al dominio l'impostazione dei criteri di gruppo che definisce il diritto utente 'Impersonare un client dopo l'integrazione'. Questo diritto utente dovrebbe essere collegato solo ad un sito o ad un'unità organizzativa (OU, organizational unit)".

Soluzione:

Consultare l'articolo Microsoft Knowledge Base ID 930220 per alcuni suggerimenti utili per ripristinare la piena connettività TCP/IP non protetta disabilitando i servizi IPSec e riavviando il computer, oltre ad alcuni passaggi per aggiungere nuovamente i gruppi Amministratori e SERVIZIO come impostazione dei criteri di gruppo. Aprire il seguente collegamento:

http://support.microsoft.com/kb/930220

Microsoft consiglia anche le seguenti procedure per risolvere i problemi causati dall'applicazione come criterio di gruppo dell'impostazione "Impersona un client dopo l'autenticazione" :

- Metodo 1: modificare le impostazioni dei criteri di gruppo
- Metodo 2: modificare il registro di sistema

Consultare l'articolo Microsoft Knowledge Base ID 911801 per i passaggi utili per implementare entrambe le soluzioni consigliate. Aprire il seguente collegamento:

http://support.microsoft.com/kb/911801

L'abilitazione della comunicazione SSL causa ritardi ODBC/JDBC

Sintomo:

Quando la comunicazione agente-server CA Enterprise Log Manager è in modalità Non FIPS, l'abilitazione della comunicazione SSL provoca una breve interruzione nella comunicazione ODBC/JDBC.

Soluzione:

Se si utilizza ODBC o JDBC, il server CA Enterprise Log Manager potrebbe non essere in grado di comunicare immediatamente quando si abilita SSL. Attendere cinque minuti circa per consentire un ripristino della comunicazione.

Le integrazioni del sensore log del file 4.0.0.0 NON supportano SUSE Linux

Sintomo:

Dopo l'aggiornamento diretto da CA Enterprise Log Manager versione 12.1 alla versione 12.1 SP1, viene visualizzata un'istruzione incorretta in merito al supporto della piattaforma nell'assistente di integrazione. Se si seleziona la versione 4.0.0.0 del sensore log di file nel primo passaggio della procedura guidata, la piattaforma "Linux_X86_32 SLES11" verrà visualizzata nell'elenco delle piattaforme disponibili.

Soluzione:

Questa informazione è incorrette, in quanto la piattaforma SUSe Linux non è supportata per il sensore log di file 4.0.0.0. Ignorare questa istruzione. Non è, quindi, possibile creare un'integrazione personalizzata utilizzando questo sensore di log.

Limitazione alla configurazione delle porte

Sintomo:

Quando il listener di syslog è configurato con la porta UDP predefinita su un agente in esecuzione come utente non di root su un host Linux, la porta UDP 514 (predefinita per syslog) non viene aperta e su di essa non viene raccolto nessun evento syslog.

Soluzione:

Se l'agente è in esecuzione come utente non di root su un sistema UNIX, modificare le porte del listener di syslog su numeri di porta superiori a 1024 o modificare il servizio per l'esecuzione come root.

Se sono selezionate troppe integrazioni, le prestazioni potrebbero diminuire

Sintomo:

Le prestazioni dell'agente predefinito diminuiscono se si specificano troppe integrazioni syslog predefinite per un connettore. In questo caso, le prestazioni fanno riferimento al numero di eventi gestiti al secondo (eps).

Soluzione:

Per ciascuna integrazione, CA Enterprise Log Manager carica i file di analisi dei messaggi (XMP) ed i file di mapping dei dati (DM). Durante le operazioni, CA Enterprise Log Manager verifica gli eventi in arrivo in base agli elenchi di espressioni regolari. Un numero elevato di file indica tempi di elaborazione più lunghi.

Evitare prestazioni rallentate tramite la rimozione delle integrazioni non necessarie durante la creazione di un connettore syslog. Dopo l'installazione, rivedere le integrazioni configurate per il connettore syslog predefinito e rimuovere quelle non necessarie.

La rimozione di un server dalla federazione non rimuove l'agente predefinito

Sintomo:

Quando si rimuove un server CA Enterprise Log Manager da un gruppo di server federati, l'agente predefinito del server eliminato non viene rimosso dal relativo gruppo di agenti.

Soluzione:

Eliminare manualmente l'agente dal suo gruppo nella sottoscheda Explorer agente.

I rapporti con dati raccolti dal SAPI collector CA non visualizzano correttamente gli eventi

Sintomo:

Negli eventi raccolti mediante il SAPI collector CA Audit i campi non sono popolati correttamente. Questo fa sì che nella maggior parte dei rapporti i dati non vengano visualizzati nel modo previsto.

Soluzione:

Utilizzare il SAPI router CA Audit per raccogliere eventi dall'infrastruttura CA Audit.

Ulteriori informazioni sulla configurazione del router SAPI sono disponibili nella sezione Considerazioni per utenti di CA Audit della *Guida all'implementazione*.

Il recapito syslog su UDP non è garantito

Sintomo:

Il recapito garantito può essere un problema per la raccolta diretta di syslog mediante il protocollo UDP del listener di syslog.

Soluzione:

Si consideri l'impiego di un meccanismo di raccolta locale di syslog come soluzione per i potenziali problemi con il recapito garantito. Ossia, configurare un listener di syslog su un agente installato con l'origine evento syslog.

Nota: utilizzare la porta per syslog, 514, solo se l'agente è in esecuzione come root. Se l'agente è in esecuzione come agente con privilegi inferiori, come consigliabile, assegnare una porta privata. Le porte private sono quelle comprese tra 49152 e 65535.

Conflitto con i servizi syslog su UNIX

Sintomo:

CA Enterprise Log Manager non riceve eventi syslog nel seguente scenario:

Computer 1

Un server CA Enterprise Log Manager in attesa di eventi syslog da Computer 2.

Computer 2

Un computer RHEL 4.0 con un agente locale contenente un connettore syslog e che invia i propri eventi a Computer 1 mediante il listener di syslog.

Computer 3

Un computer UNIX che invia eventi a Computer 2 mediante il connettore installato su quest'ultimo.

In questo caso, il computer dell'agente non è in grado di acquisire gli eventi da Computer 3 in quanto il servizio syslog del sistema operativo ed il connettore syslog sono in esecuzione sullo stesso sistema.

Soluzione:

Arrestare il servizio syslog su Computer 2 per ricevere eventi da Computer 3 (il computer UNIX). È anche possibile riconfigurare l'ambiente in modo da evitare conflitti dei servizi syslog sul medesimo computer.

Il sensore di registro WMI genera più eventi con privilegi utente

Sintomo:

Quando si usa un connettore con il sensore di registro WMI per raccogliere eventi, si potrebbero verificare più eventi correlati all'"uso del privilegio".

Soluzione:

Questi eventi vengono visualizzati se sul sistema di destinazione è abilitato il criterio di controllo Windows che registra con successo le azioni di uso del privilegio. Questi sono una conseguenza del processo di raccolta dell'evento e non indicano la presenza di alcun problema. Se non si desidera visualizzarli, è possibile creare una regola di soppressione per interromperne la ricezione da parte di CA Enterprise Log Manager.

Interruzione della ricezione di eventi da parte del sensore log di file di testo in esecuzione su un sistema agente Solaris.

Sintomo:

Il sensore log di file di testo in esecuzione su un sistema agente Solaris interrompe la ricezione degli eventi.

Il file di log del connettore contiene un errore che indica che non è stato possibile aprire il file di libreria libssl.so.0.9.7:

```
[4] 07/20/10 18:55:50 ERROR :: [ProcessingThread::DllLoad] :Error is: ld.so.1:
caelmconnector: fatal: libssl.so.0.9.7: open failed: No such file or directory
[4] 07/20/10 18:55:50 ERROR :: [ProcessingThread::run] Dll Load and Initialize
failed, stopping the connector ...
[3] 07/20/10 18:55:50 NOTIFY :: [CommandThread::run] Cmd_Buff received is START
```

Soluzione:

Individuare la posizione della libreria per abilitare l'agente alla ricezione degli eventi.

Per risolvere l'errore sul sistema agente Solaris

1. Accedere alla cartella /etc. Ad esempio:

   ```
   cd /etc
   ```

2. Aprire il file di profilo nella cartella etc: Ad esempio:
   ```
   vi /etc/profile
   ```

3. Aggiungere le seguenti due righe alla fine del file di profilo:

   ```
   LD_LIBRARY_PATH=/usr/sfw/lib:$LD_LIBRARY_PATH
   ```

   ```
   export LD_LIBRARY_PATH
   ```

4. Chiudere la sessione corrente del sistema agente Solaris.
5. Aprire una nuova sessione nel sistema agente Solaris.
6. Interrompere l'agente CA Enterprise Log Manager sul sistema Solaris. Ad esempio:

   ```
   /opt/CA/ELMAgent/bin/S99elmagent stop
   ```

7. Avviare l'agente CA Enterprise Log Manager sul sistema Solaris. Ad esempio:

   ```
   /opt/CA/ELMAgent/bin/S99elmagent start
   ```

   Il sensore log di file di testo inizia a ricevere eventi ed il messaggio di errore non viene più visualizzato nel file di log.

Capacità di risposta nulla dell'agente causata da un flusso di eventi eccessivo

Sintomo:

Un agente CA Enterprise Log Manager smette di rispondere ed interrompe la ricezione degli eventi. Il seguente messaggio di errore viene visualizzato nel file caelmdispatcher.log:

```
[275] 07/12/10 14:32:05 ERROR :: FileQueue::PutEvents Unable to write to new event file
[275] 07/12/10 14:32:05 ERROR :: WriterThread::run Unable to push events to FileQueue, Retrying
[275] 07/12/10 14:32:10 NOTIFY :: FileQueue::UpdateCurrentWriterFile Reached Max files configured limit=10, Not creating any new files for now
```

Soluzione:

Tale comportamento indica che il tasso di eventi in arrivo per l'hardware nell'ambiente è elevato. È possibile risolvere il problema riconfigurando l'agente mediante le seguente procedura:

1. Fare clic su Amministrazione, sulla scheda secondaria Raccolta log ed espandere la cartella Gestione agenti.
2. Selezionare l'agente che si desidera riconfigurare, fare clic su Modifica ed impostare i seguenti parametri:

   Numero massimo di file

   Consente di impostare il numero massimo di file che possono essere creati nella coda di file di ricezione degli eventi. Il numero massimo consentito corrisponde a 1000 file. L'impostazione predefinita è 10.

   Dimensioni massime per file

   Consente di impostare la dimensione massima (in MB) per ciascun file nella coda di file di ricezione degli eventi. Quando un file raggiunge la dimensione massima, CA Enterprise Log Manager crea un nuovo file. La dimensione massima consentita è 2048 MB. L'impostazione predefinita corrisponde a 100 MB.

   È possibile regolare questi parametri in un secondo momento in base alle esigenze del proprio ambiente ed in base alla percentuale di eventi al secondo.

Dispositivo (non UI)

Quelli descritti di seguito sono i problemi noti relativi al dispositivo software (non all'interfaccia utente di CA Enterprise Log Manager).

Impossibile accedere al server CA Enterprise Log Manager con il nome utente EiamAdmin

Sintomo:

Il nome utente e la password dell'utente EiamAdmin non vengono riconosciuti quando si tenta di accedere al server CA Enterprise Log Manager (non attraverso l'interfaccia utente).

Soluzione:

Per eseguire attività di manutenzione, come la configurazione dell'archiviazione, l'installazione crea un altro nome utente, caelmadmin, e gli assegna la stessa password del programma di installazione fornito per EiamAdmin. Utilizzare il nome utente caelmadmin e la relativa password per accedere al server CA Enterprise Log Manager.

Per ulteriori informazioni, consultare Account utente predefiniti nella *Guida all'implementazione*.

Numero eccessivo di file di registro ELMAdapter

Sintomo:

Sul server CA Enterprise Log Manager è possibile accumulare un numero elevato di file di registro Adapter. Questa è una situazione atipica, in cui la regola sarebbe aggiungere messaggi di registro in un unico file di registro. Tale problema può essere causato dall'attivazione del tracciamento.

Come determinare la presenza del problema

1. Pianificare rapporti e avvisi ed eseguire query ODBC, come riportato di seguito:

   ```
   Selezionare event_logname,count(*) from view_event where event_time_gmt >=
   timestampadd(hh,-1,now()) AND event_time_gmt <= now() group by event_logname;
   ```

2. Accedere al server CA Enterprise Log Manager utilizzando SSH e fornire il nome utente e la password di caelmadmin.
3. su per passare a root e fornire la password di root.
4. Andare alla cartella iTechnology:

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

5. Determinare se, a causa dell'esecuzione della query tramite i driver ODBC; è stato creato un numero eccessivo di file di registro. Questi file sono denominati ELMAdapter_<oaserverpid>_-IP.log.

Soluzione:

Nel caso in cui si presenti tale problema, assicurarsi che il tracciamento degli errori sia disabilitato:

1. accedere al server di gestione CA Enterprise Log Manager utilizzando SSH e fornire il nome utente e la password di caelmadmin.
2. su per passare a root e fornire la password di root.
3. Andare alla cartella iTechnology:

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

4. Aprire oaserver-dm.ini per effettuare le modifiche.
5. Scorrere fino a [Service_0] e assicurarsi che il tracciamento sia impostato su disabilitato. In caso contrario, modificare l'impostazione come indicato nell'esempio seguente:

   ```
   ServiceDebugLogLevel=0
   ServiceIPLogOption=Disable All Tracing
   ```

6. Riavviare il Servizio ODBC come segue:
   a. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
   b. Fare clic su Server ODBC.

c. Eseguire una delle seguenti operazioni:

- Se Abilita servizio non è selezionato, selezionarlo e fare clic su Salva.
- Se Abilita servizio è selezionato, deselezionare la casella di controllo Abilita servizio, fare clic su Salva, selezionare Abilita servizio e fare di nuovo clic su Salva.

L'importazione manuale dei file di analisi potrebbe richiedere la modifica dei valori del timeout.

In alcuni casi, quando si importano file di analisi (.XMP) durante l'installazione CA Enterprise Log Manager si verificano dei problemi. Tale problema si verifica con maggiore frequenza quando l'installazione CA Enterprise Log Manager avviene su server che non soddisfano i requisiti minimi di hardware o su reti lente.

Sintomo:

Durante l'installazione, si verifica un errore nell'importazione dei file di analisi. È possibile risolvere il problema una volta terminata l'installazione. È sufficiente eseguire lo script fornito, *EEM/content/ImportCALMXMP.sh,* per importare i file manualmente. (Ulteriori informazioni su questo script sono disponibili nella *Guida all'implementazione*.) In genere, eseguendo questa azione si risolve il problema.

A volte, tuttavia, mentre si esegue lo script di importazione manuale, il tentativo di importazione del file Cisco Router XMP può fallire. L'installazione del server CA Enterprise Log Manager è riuscita. Tuttavia l'errore di importazione del file XMP provoca un'installazione errata dei connettori predefiniti sull'agente locale. Non è possibile distribuire i connettori finché l'importazione manuale dei file XMP non viene eseguita con successo.

Soluzione:

Il superamento di un valore predefinito di timeout nello script *EEMImportUtility.sh* causa problemi durante l'importazione del file Cisco XMP. Lo script *ImportCALMXMP.sh* richiama lo script *EEMImportUtility.sh*. Il valore predefinito per il timeout è 4 minuti. Impostare il timeout predefinito a 6 minuti per concedere il tempo necessario all'importazione manuale su server più lenti.

Per modificare il valore predefinito di timeout

1. Accedere alla directory EEM/content.
2. Modificare il file ImportCALMXMP
3. Individuare la riga seguente e modificare il valore di timeout come illustrato di seguito:

   ```
   ./EEMImportUtility.sh -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP" to "./EEMImportUtility.sh -timeout 360000 -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP
   ```

   Nota: il valore di timeout è espresso in millisecondi.
4. Salvare e chiudere il file.
5. Eseguire di nuovo lo script.
6. Distribuire manualmente i connettori sia per syslog che per Linux_LocalSyslog sull'agente predefinito.

Perfezionamento eventi

Quelli descritti di seguito sono i problemi noti relativi al perfezionamento degli eventi.

I valori stringa e numerici di mapping di blocco richiedono operatori diversi

Sintomo:

Quando si utilizza la procedura guidata di mapping, i valori di mapping di blocco per le colonne con stringhe numeriche o di testo potrebbero non rispondere come previsto.

Soluzione:

Quando si creano dei mapping di blocco, l'operatore "Equal" può essere usato solo con le colonne numeriche. Utilizzare l'operatore Match per tutte le colonne di stringhe di testo.

Il mapping dei dati personalizzato non è in grado di mappare eventi epSIM (iTech)

Sintomo:

Il file di mapping dei dati (DM) creato per eventi epSiM (iTechnology) non è in grado di eseguire il mapping degli eventi dopo essere stato applicato al plugin iTechnology eventplugin scheda nella Gestione raccolta log.

Quando si analizza la query Tutti gli eventi iTech per determinare se gli eventi sono mappati in base al file DM personalizzato, gli eventi iTech non vengono mappati e, quindi, non vengono restituiti come risultato della query. Viene, quindi, visualizzato il messaggio "Non è stato eseguito il mapping di nessun evento. Impossibile eseguire il mapping degli eventi".

Soluzione:

Aprire il file DM personalizzato e sostituire $EventLog con $Log. Ovvero,

Modificare la riga: <DM_Field name="event_logname" type="string" value="$EventLog" mapping="direct"/>

Con: <DM_Field name="event_logname" type="string" value="$Log" mapping="direct"/>

Questa modifica assicura che gli eventi vengano mappati. Durante l'analisi del mapping, ignorare eventuali messaggi successivi del tipo: "Non è stato eseguito il mapping di nessun evento".

Query e rapporti

Quelli descritti di seguito sono i problemi noti relativi alle query ed ai rapporti.

I risultati della query di avviso possono essere incompleti.

Sintomo:

Quando viene generato un avviso, è possibile visualizzare immediatamente in CA Enterprise Log Manager il risultato della query. Per visualizzare i risultati in CA Enterprise Log Manager, fare clic sulla scheda Gestione avvisi, nella sottoscheda Avvisi, e quindi selezionare il nome dell'avviso. I risultati vengono visualizzati sotto forma di diagramma. Quando l'avviso richiama un processo CA IT PAM di output evento/avviso che apre un ticket dell'help desk su CA Service Desk, verrà visualizzato un URL nel problema di help desk. Selezionando l'URL ed effettuando l'accesso, i risultati della query relativi all'avviso verranno visualizzati su un'unica pagina. Se si confrontano questi risultati con quelli visualizzati sulla sottoscheda Avvisi, si potrebbe notare una mancata corrispondenza dei risultati della query. Ad esempio, se i risultati vengono visualizzati per Numero, i numeri visualizzati nell'URL potrebbero risultare superiori a quelli visualizzati in CA Enterprise Log Manager. Tale problema si verifica su sistemi con notevole carico di lavoro quando l'ora di fine dinamica impostata nelle Condizioni di risultato dell'avviso risulta inadeguata. Un'impostazione è considerata inadeguata quando non fornisce il tempo necessario per effettuare l'aggiornamento del database prima che questo venga letto. La probabilità che ciò si verifichi è stata ridotta impostando l'ora di fine dinamica predefinita su 'ora' e l'intervallo predefinito Ultimi 5 minuti su '2 minuti'.

Soluzione:

Modificare l'ora di fine dinamica dell'avviso nel passaggio Condizioni di risultato da 'ora', '-2 minuti' a un valore maggiore, come 'ora', '-10 minuti'.

Limitazione alle query con più termini di ricerca

Sintomo:

Una query su una singola colonna di ricerca esegue, come previsto, una ricerca senza distinzione tra maiuscole e minuscole. Invece, una query su più colonne di ricerca esegue una ricerca con distinzione tra maiuscole e minuscole in cui gli asterischi (*), generalmente interpretati come caratteri jolly, vengono invece interpretati letteralmente. Questo problema si verifica quando il codice SQL generato internamente contiene l'operatore OR nella clausola Where.

Soluzione:

Limitare le proprie query alle ricerche su una colonna alla volta quando si usano i prompt. Se si crea una propria query con più espressioni, connettere più espressioni con caratteri jolly LIKE con l'operatore logico, AND.

Impossibile applicare un filtro semplice alla procedura guidata per la query in presenza di caratteri speciali

Sintomo:

I filtri semplici della procedura guidata per la query riportano errore quando nel valore del campo relativo al filtro semplice vengono digitati caratteri speciali. È possibile salvare ed eseguire la query con i seguenti caratteri speciali:

```
( ) & * > < ? : } {
```

Tuttavia, la query viene eseguita senza introdurre quel campo come filtro e i dati vengono visualizzati anche se le condizioni non vengono soddisfatte.

Soluzione:

Non utilizzare i caratteri speciali riportati in elenco come parte dei valori del campo relativo al filtro semplice.

Stato del processo pianificato non visualizzato dopo l'aggiornamento

Sintomo:

Sulla scheda Rapporti pianificati, sottoscheda Pianificazione rapporto, è possibile visualizzare tutti i processi pianificati con il relativo stato. La colonna Stato visualizza Generazione in corso durante il processo di generazione del rapporto e Pianificato quando il processo è pianificato. Dopo un aggiornamento dalla versione base r12.0 GA, la colonna Stato dei rapporti viene cancellata, indipendentemente dallo stato. Quando un rapporto pianificato viene rigenerato, il suo stato torna ad essere visualizzato.

Soluzione:

L'omissione di un valore nella colonna Stato relativa a un processo pianificato è un problema di visualizzazione temporaneo. Non intraprendere alcuna azione. Lo stato corretto verrà visualizzato alla successiva generazione del rapporto.

Alcuni processi di avviso non riescono se pianificati con ricorrenza frequente

Sintomo:

Quando un avviso che interroga eventi generati durante un intervallo di tempo dato viene pianificato con una frequenza di esecuzione superiore a tale intervallo, i processi possono sovrapporsi e non riuscire. Viene visualizzato, quindi, il seguente messaggio indicante che l'avviso non può essere generato poiché è in corso una query precedente. Ad esempio, se si desidera eseguire una query per eventi specifici generati durante le ultime tre ore, ma impostarla per essere eseguita ogni ora, il primo processo non potrà essere completato prima che il secondo abbia inizio. In tal caso, CA Enterprise Log Manager continua l'elaborazione del primo processo pianificato e invia i messaggi di errore per gli altri due processi successivi pianificati. Non appena terminato l'intervallo di 3 ore, viene inviato un avviso se si sono verificati gli eventi che soddisfano i criteri della query e ha inizio la successiva esecuzione dell'avviso.

Soluzione:

Se si specifica solo una Selezione intervallo date nel passaggio Condizioni di risultato, selezionare un intervallo di ricorrenza *uguale* all'intervallo impostato per il campo Selezione intervallo date. Ad esempio, se si desidera eseguire una query per gli eventi che soddisfano criteri specifici generati durante le ultime tre ore, impostare la Selezione intervallo date nel passaggio Condizioni di risultato come segue:

Ora di fine dinamica: 'now' '-2 minutes'

Ora di inizio dinamica: 'now' '-182 minutes'

Quando si definisce la pianificazione, è necessario impostare l'intervallo di ricorrenza nel passaggio Pianifica processi per un valore pari a 3 ore (180 minuti), come indicato di seguito:

Intervallo di ricorrenza: 3 ore

Impostare lo stesso intervallo di query e di ricorrenza assicura che ciascuna occorrenza dell'evento che soddisfi i criteri di query venga registrata in un avviso generato. Lo stesso vale per intervalli di tempo specificati per eventi raggruppati.

Impossibile eliminare i tag contenenti caratteri speciali

Sintomo:

Tentativi di eliminazione di una query o di tag di rapporto contenenti i caratteri speciali, ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ? non riusciti.

Soluzione:

Non utilizzare i caratteri speciali considerati durante la creazione di query o di tag di rapporto.

Sottoscrizione

Quelli descritti di seguito sono i problemi noti relativi alla sottoscrizione.

Riavvio automatico dopo l'aggiornamento del sistema operativo durante l'aggiornamento del Service Pack

Sintomo:

Se l'opzione di sottoscrizione "Riavvio automatico dopo l'aggiornamento del sistema operativo" è impostata su Sì quando si applica l'aggiornamento del Service Pack, il sistema operativo si riavvia prima del completamento dell'aggiornamento dei file binari di CA Enterprise Log Manager. Un aggiornamento lasciato incompleto è quello degli script di arresto di iGateway. Questo aggiornamento dev'essere applicato in modo che iGateway possa essere arrestato normalmente al riavvio del sistema operativo.

Soluzione:

Prima di applicare l'aggiornamento del modulo Log Manager del Service Pack, accertarsi che l'opzione di sottoscrizione Riavvio automatico dopo l'aggiornamento del sistema operativo sia impostata su No.

Errore di memoria insufficiente su macchine con dotazione di memoria scarsa

Sintomo:

Il download di un aggiornamento della sottoscrizione su un computer con memoria inferiore agli 8 GB consigliati potrebbe non riuscire a causa di un errore Java di memoria insufficiente. Sono stati scaricati pacchetti di grandi dimensioni utilizzando iGateway dove non è presente l'impostazione di dimensione heap di Java Virtual Machine (JVM).

<so

Se si installa CA Enterprise Log Manager su hardware con una memoria inferiore agli 8 GB consigliati, modificare l'impostazione della dimensione heap JVM modificando il file caelm-java.group.

Per modificare l'impostazione di dimensione heap di JVM:

1. Accedere al server CA Enterprise Log Manager come caelmadmin.
2. Individuare la cartella iGateway
3. Aprire il file caelm-java.group e individuare la sezione impostazioni JVM.
4. Aggiungere la nuova riga, come illustrato di seguito in grassetto:

```
<JVMSettings>
                <loadjvm>true</loadjvm>
                <javahome>/usr/java/latest/jre</javahome>
                <Properties
name="java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed">
                        <system-
properties>java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed</
system-properties>
                </Properties>
        <Properties name="maxmemory"><jvm-property>-Xmx1250M</jvm-
property></Properties>
        </JVMSettings>
```

5. Salvare e chiudere il file caelm-java.group

Importante: l'impostazione della dimensione heap di JVM può causare problemi quando si utilizza l'opzione Esporta a PDF con i set di dati molto grandi. Questa opzione quindi è utile solo sui piccoli computer.

La modifica delle credenziali del proxy causa il blocco dell'account di dominio

Sintomo:

Le credenziali del dominio non funzionano ed il proprio account potrebbe essere bloccato in un ambiente con server CA Enterprise Log Manager.

Soluzione:

Il server CA Enterprise Log Manager contatta il server di sottoscrizione CA regolarmente per controllare se sono presenti aggiornamenti di prodotti. Se le credenziali del proxy (come ID utente e password) sono scadute o sono state modificate, CA Enterprise Log Manager non è in grado di contattare il server di sottoscrizione e genera un evento di automonitoraggio relativo all'accesso non riuscito. L'evento di automonitoraggio visualizzerà un messaggio simile al seguente:

```
Impossibile connettersi al server di contenuti di sottoscrizione. Il server è
inattivo, la connessione è stata rifiutata o le impostazioni del server proxy
sono errate. Convalidare le impostazioni del server proxy.
```

Se gli accessi non riusciti proseguono, l'account del dominio potrebbe essere bloccato, in relazione a quanto definito nei criteri locali. Accertarsi che le credenziali del proxy non siano state modificate o non siano scadute.

Si consiglia di non impostare un criterio di scadenza password per l'account di servizio impiegato per contattare il server di sottoscrizione.

L'evento di automonitoraggio per il riavvio appare solo una volta

Sintomo:

Quando si seleziona un modulo di sistema operativo da scaricare tramite sottoscrizione e si specifica l'installazione senza riavvio, l'evento di automonitoraggio seguente viene generato solo una volta: Gli aggiornamenti del sistema operativo sono stati installati su questo host. Riavviare il computer per rendere effettivi gli aggiornamenti.

Soluzione:

La sottoscrizione genera un evento che ricorda di riavviare il sistema operativo solo una volta quando è richiesto un riavvio manuale. È buona prassi creare un avviso per questo evento.

Ulteriore selezione dei moduli di sottoscrizione in seguito all'aggiornamento

Sintomo:

Durante l'aggiornamento di CA Enterprise Log Manager a r12.1, tutti i moduli di sottoscrizione selezionati precedentemente verranno spostati dall'elenco selezionato all'elenco dei moduli disponibili. L'azione previene ulteriori aggiornamenti di sottoscrizione di tali moduli.

Soluzione:

In seguito all'aggiornamento, sarà necessario selezionare i moduli da utilizzare utilizzando la seguente procedura:

Per selezionare nuovamente i moduli di sottoscrizione

1. Effettuare l'accesso a CA Enterprise Log Manager e selezionare la scheda Amministrazione, quindi selezionare la sottoscheda Servizi.
2. Aprire il modulo di sottoscrizione per ogni server di cui si desidera eseguire l'aggiornamento.
3. Utilizzando i controlli pilota della sottoscrizione e spostarei moduli che si desidera rendere disponibili per l'aggiornamento dall'elenco dei moduli disponibili all'elenco dei moduli selezionati.
4. Fare clic su Salva.

Dopo la modifica apportata alla configurazione, il pulsante Verifica proxy restituisce falsi positivi.

Sintomo:

Quando si modificano le impostazioni del server proxy CA Enterprise Log Manager e si esegue nuovamente un test utilizzando il pulsante Verifica proxy dopo aver completato correttamente una verifica, verrà visualizzato un messaggio di conferma che segnalerà se la configurazione è stata completata correttamente o meno.

Soluzione:

Il pulsante Verifica proxy usa la configurazione proxy specificata per accedere ad un URL tramite lo stesso proxy. In genere, se validi, i server proxy inseriscono nella cache l'autenticazione del client ed ignorano le credenziali successive fino allo scadere del tempo di inattività.

Ciò significa che, una volta che il pulsante Verifica proxy avrà correttamente indicato la validità della configurazione, le successive verifiche di eventuali configurazioni non corrette verranno erratamente visualizzate come valide per un certo periodo di tempo.

Errore durante l'applicazione di due regole di soppressione

Sintomo:

Le seguenti regole di soppressione, appartenenti a r12.0, non vengono applicate correttamente:

- TMCM - Notifiche di corretto completamento dell'aggiornamento del modulo e delle impronte digitali del virus
- Notifiche di corretto completamento dell'aggiornamento del modulo e dell'impronta digitale del virus McAfee

Soluzione:

Le regole non vengono applicate correttamente nelle lingue in cui viene utilizzato il simbolo &. Nella versione 12.1 sono state apportate le seguenti modifiche alle regole:

- TMCM - Notifiche di corretto completamento dell'aggiornamento del modulo e delle impronte digitali del virus
- Notifiche di corretto completamento dell'aggiornamento del modulo e dell'impronta digitale del virus McAfee

Utilizzare le nuove regole senza il simbolo &.

Per effettuare l'aggiornamento a r12.1, è necessario riavviare iGateway

Sintomo:

In un ambiente federato, l'aggiornamento da r12.0 a r12.1 non viene completato senza riavviare iGateway.

Soluzione:

Gli aggiornamenti binari vengono copiati ed estratti dal client di sottoscrizione, ma non vengono installati: rimangono quindi tali e quali nella directory "/tmp/downloads". Questo indica che il processo di aggiornamento della Sottoscrizione non è stato completato. A questo punto, occorre riavviare manualmente igateway tramite la procedura seguente:

Per riavviare il daemon o il servizio iGateway

1. Accedere come utente caelmadmin per il server CA Enterprise Log Manager.
2. Commutare gli utenti sull'account root tramite il seguente comando:

   ```
   su -
   ```

3. Terminare il processo igateway con il seguente comando:

   ```
   $IGW_LOC/S99igateway stop
   ```

4. Avviare il processo iGateway con il comando seguente:

   ```
   $IGW_LOC/S99igateway start
   ```

Questo consentirà di completare l'aggiornamento.

L'aggiornamento alla versione r12.1 SP1 potrebbe richiedere il riavvio di iGateway

Sintomo:

l' aggiornamento dalla versione r12.1 alla versione r12.1 SP1 potrebbe non essere completato entro il tempo massimo consentito. Se il processo di sottoscrizione viene eseguito per un'ora e mezza o più senza essere completato, potrebbe essere necessario un riavvio di iGateway.

Soluzione:

Per identificare il problema, si consiglia di utilizzare la seguente procedura:

1. Completare la sottoscrizione al contenuto (rapporti e integrazioni) dalla versione 12.1 GA.
2. Completare la sottoscrizione al file binario (moduli server, agente, OS) dalla versione SP1.

Ciò consentirà di distinguere il tempo impiegato per il download di ciascun modulo, poiché il tempo può variare a seconda delle dimensioni del modulo. Se la parte relativa alla sottoscrizione dura troppo a lungo senza poter essere completata, riavviare iGateway dall'interfaccia utente CA Enterprise Log Manager.

Per riavviare il servizio iGateway:

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Espandere la voce Stato del sistema.
3. Selezionare un server CA Enterprise Log Manager.
4. Fare clic sulla scheda Amministrazione.
5. Fare clic su Riavvia iGateway.

L'aggiornamento del sensore log syslog alla versione r12.1 SP1 richiede l'aggiornamento delle integrazioni sugli agenti Windows

Sintomo:

Se non viene applicato l'aggiornamento del modulo Integrazioni al momento dell'aggiornamento alla versione r12.1 SP1, i connettori che utilizzano il sensore log syslog smetteranno di funzionare. Nel file di log dell'agente viene visualizzato il seguente errore:

```
[6072] 03/09/10 17:22:51 ERROR :: MySAX2Handler::fatalError: at line1
[6072] 03/09/10 17:22:51 ERROR :: XMLTree::ParseUsingSAX2:error parsing
stringintruvert/jsp/admin/Login.jsp
[6072] 03/09/10 17:22:51 ERROR :: XMLTree::Parse Exit ParseUsingSAX2 FAILURE
[6072] 03/09/10 17:22:51 ERROR :: HTTP_Processor::ParseRequestXML: Unknown
request format:intruvert/jsp/admin/Login.jsp
```

Si consiglia di verificare anche la versione dell'integrazione. Se tale versione è precedente alla 12.1.5104.0, è necessario applicare l'aggiornamento.

Soluzione:

Applicare l'aggiornamento del modulo Integrazioni, quindi aggiornare ciascuna integrazione che utilizza il sensore log syslog alla versione 12.1.5104.0 o successive. In alternativa, eseguire i passaggi riportati nella *Guida all'amministrazione*nella sezione relativa all'aggiornamento delle configurazioni di più connettori.

Per un elenco delle integrazioni che utilizzano il sensore log syslog, consultare la Matrice di integrazione del prodotto CA Enterprise Log Manager all' indirizzo https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.html.

Gestione utenti e accessi

Quelli descritti di seguito sono i problemi noti relativi alla gestione di utenti e accessi.

Limitazioni di accesso da un browser in Windows Vista

Sintomo:

Quando si accede a CA Enterprise Log Manager da computer con sistema operativo Windows Vista SP1 abilitato a IPv6 da qualunque browser, non sarà possibile accedere alle funzionalità attraverso i pulsanti della sottoscheda Gestione utenti e accessi della scheda Amministrazione.

Gli utenti che accedono con le credenziali EiamAdmin o con quelle di un account utente di CA Enterprise Log Manager cui sia stato assegnato il ruolo Amministratore dovrebbero riuscire ad accedere a questa funzionalità. Questa limitazione non si applica agli utenti che accedono a CA Enterprise Log Manager tramite un browser da un qualunque altro sistema operativo Windows. Essa vale solo per l'accesso a CA Enterprise Log Manager tramite browser con un URL nel formato seguente da un computer Windows Vista https://[*indirizzo ipv6*]:5250/spin/calm. Un esempio è il seguente URL:

`https://[::FFFF:192.168.00.00]:5250/spin/eiam`

Soluzione:

Per risolvere questo problema è sufficiente accedere alla funzionalità Gestione utenti e accessi attraverso un URL diverso.

1. Immettere l'URL seguente nel proprio browser, dove l'indirizzo IPv6 è l'URL del proprio server di gestione CA Enterprise Log Manager.

   `https://[`*`indirizzo ipv6`*`]:5250/spin/eiam`

2. Selezionare CAELM dall'elenco a discesa Applicazione.
3. Nei campi Nome utente e Password, immettere EiamAdmin con la password di questo account o le credenziali di un utente CA Enterprise Log Manager con il ruolo Amministratore.
4. Fare clic sulla scheda Gestione identità per configurare utenti e gruppi.
5. Fare clic sulla scheda Gestione criteri di accesso per configurare test o calendari.
6. Fare clic sulla scheda Configurazione, EEM server per configurare utenti globali, gruppi globali o criteri password.

Limitazione all'uso del calendario con i criteri di accesso

Sintomo:

Si dispone dell'accesso utente o di gruppo limitato a CA Enterprise Log Manager durante gli orari e i giorni specificati su un calendario con un criterio che concede esplicitamente l'accesso. Tuttavia, il calendario non funziona come previsto con un criterio che nega esplicitamente l'accesso.

Soluzione:

Utilizzare il tipo criterio di accesso esplicito per limitare le ore in cui si desidera concedere l'accesso ad un gruppo, anziché usare un criterio di negazione esplicita.

Varie

Quelli che seguono sono vari problemi noti.

CA Enterprise Log Manager a volte non risponde

Sintomo:

A volte CA Enterprise Log Manager non risponde. Ossia, l'interfaccia utente non risponde alle richieste dell'utente e le richieste interne dall'agente a Gestione agente si interrompono. La raccolta dei registri tuttavia continua.

Soluzione:

Utilizzare la seguente procedura per terminare il processo iGateway e riavviarlo:

1. Accedere al server CA Enterprise Log Manager che non risponde attraverso ssh in qualità di utente caelmadmin.
2. Commutare gli utenti sull'account root tramite il seguente comando e fornire la password di root:

   ```
   su -
   ```

3. Passare alla directory $IGW_LOC.

   Per impostazione predefinita, iGateway risiede nella directory /opt/CA/SharedComponents/iTechnology.

4. Interrompere il processo iGateway con il comando seguente:

   ```
   ./S99igateway stop
   ```

5. Avviare il processo iGateway con il comando seguente:

   ```
   ./S99igateway start
   ```

Query API e chiamate di rapporto non riescono su alcuni browser

Sintomo:

Quando si utilizza Open API getQueryViewer o getReportViewer su Microsoft Internet Explorer 7 o 8 o su Mozilla Firefox, non viene visualizzato alcun risultato.

Soluzione:

Nei browser specificati, l'API di CA Enterprise Log Manager non riesce a riconoscere il parametro "server" nell'URL di chiamata API. Per evitare questo problema, non specificare un parametro server nelle chiamate getQueryViewer o getReportViewer. Quando viene visualizzata l'interfaccia CA Enterprise Log Manager, selezionare il server desiderato dall'elenco a discesa dei server Log Manager collocato nella parte superiore della pagina principale.

Per ulteriori informazioni sugli URL di chiamata API, consultare la *Guida alla programmazione API di CA Enterprise Log Manager*.

Supporto per CAELM4Audit non più disponibile

CA Enterprise Log Manager r12.1 SP1 utilizza CA EEM r8.4 SP3, non certificato per l'utilizzo con CA Audit. L'integrazione tra CA Enterprise Log Manager e CA Audit richiede la condivisione del server CA EEM, per cui CA Audit verrà eseguito in una configurazione non supportata.

Inoltre, CA Audit non è compatibile con FIPS e il passaggio di CA Enterprise Log Manager alla modalità FIPS determina un arresto dell'interfaccia utente di amministrazione di Audit.

Impatto del nome dell'applicazione personalizzato sulla query di archiviazione

Sintomo:

In genere, in un ambiente con più server CA Enterprise Log Manager che utilizzano lo stesso server di gestione, una query di archiviazione restituisce solitamente risultati estratti dalle directory di archiviazione di tutti i server. Tuttavia, se quando si installa il CA Enterprise Log Manager di gestione si imposta un nome di applicazione personalizzato anziché quello predefinito, cioè CAELM, la query di archiviazione non funzionerà come previsto. Piuttosto, la query di archiviazione restituirà risultati esclusivamente in relazione al server su cui la query è in esecuzione. I risultati provenienti da altri server vengono visualizzati come *<host>User CERT-custom: Accesso negato*.

Soluzione:

Eseguire la query sul catalogo archiviazioni di ciascun server CA Enterprise Log Manager separatamente.

Impostazioni a contrasto elevato per il monitor

Sintomo:

In Windows, l'unica impostazione ad alto contrasto supportata è Nero a contrasto elevato; le altre tre opzioni ad alto contrasto non sono supportate. Tra le opzioni a contrasto elevato ci sono Contrasto elevato 1, Contrasto elevato 2, Nero a contrasto elevato e Bianco a contrasto elevato.

Soluzione:

Selezionare l'impostazione Nero a contrasto elevato quando è necessaria un'impostazione a contrasto elevato. Per impostare questa opzione, selezionare Schermo dal Pannello di controllo. Questa opzione di accesso facilitato viene impostata nella finestra di dialogo Proprietà dello Schermo, scheda Aspetto, elenco a discesa Combinazione colori.

iGateway continua ad arrestarsi e riavviarsi

Sintomo:

L'interfaccia di CA Enterprise Log Manager di tanto in tanto smette di rispondere durante le operazioni. Un controllo del server CA Enterprise Log Manager rivela che il processo iGateway si arresta e si riavvia, ma non riesce a rimanere in esecuzione. Utilizzare il processo seguente per controllare il processo iGateway:

1. Accedere a un prompt dei comandi sul server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Commutare gli utenti sull'account root tramite il seguente comando:

   ```
   su - root
   ```

4. Utilizzare il comando seguente per verificare che il processo iGateway sia in esecuzione:

   ```
   ps -ef | grep igateway
   ```

   Il sistema operativo restituisce le informazioni del processo iGateway ed un elenco dei processi in esecuzione sotto iGateway.

Soluzione:

Per risolvere il problema, procedere come segue:

1. Passare a $IGW_LOC (/opt/CA/SharedComponents/iTechnology), ed individuare il file seguente:

   ```
   saf_epSIM.*
   ```

   Esistono diverse versioni numerate in sequenza, ad esempio: saf_epSIM.1, saf_epSIM.2, saf_epSIM.3 e così via.

2. Rinominare il file con il numero inferiore e salvarlo in un'altra posizione per trasmetterlo all'assistenza CA.
3. Se iGateway non si riavvia automaticamente, riavviarlo:
   a. Effettuare l'accesso come utente root.
   b. Aprire una finestra del prompt dei comandi, quindi immettere il seguente comando:

      ```
      /opt/CA/SharedComponents/iTechnology/S99igateway start
      ```

Lo spazio su disco massimo per CA Enterprise Log Manager virtuale è insufficiente

Sintomo:

Impossibile creare una macchina virtuale con uno spazio su disco allocato di 512 GB in VMware ESX Server v3.5. Il server CA Enterprise Log Manager virtuale ha bisogno di più dei 256 GB massimi per gestire il volume degli eventi.

Soluzione:

Il server VMWare ESX utilizza una dimensione di blocco predefinita di 1 MB e calcola lo spazio su disco massimo utilizzando questo valore. Quando la dimensione di blocco è impostata a 1 MB, lo spazio su disco massimo predefinito è 256 GB. Se si desidera configurare più di 256 GB di spazio su disco virtuale, è possibile aumentare la dimensione di blocco predefinita.

Per creare un disco virtuale più grande

1. Accedere alla console di servizio sul server VMware ESX.
2. Aumentare la dimensione di blocco a 2 MB con il comando seguente:

   ```
   vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   In questo comando, il valore 2M significa 512 GB (2 x 256).
3. Riavviare il server VMware ESX.
4. Creare una nuova macchina virtuale con lo spazio su disco impostato a 512 GB.

È possibile trovare maggiori informazioni su questo ed altri comandi nella documentazione del server VMware ESX.

L'aggiornamento dei registri del browser disconnette l'utente da CA Enterprise Log Manager

Sintomo:

L'aggiornamento del proprio browser mentre si è connessi a CA Enterprise Log Manager comporta la chiusura della sessione e la disconnessione dell'utente.

Soluzione:

CA Enterprise Log Manager non supporta l'aggiornamento del browser a causa delle limitazioni di Flex. Evitare di aggiornare il browser.

Possibili errori di servizio o dell'interfaccia di gestione dopo il riavvio di iGateway

Sintomo:

Facendo clic su un oggetto nei servizi dell'interfaccia o nelle strutture di gestione di CA Enterprise Log Manager subito dopo un riavvio di iGateway, è possibile che, invece del contenuto richiesto, venga visualizzato un messaggio di errore indicante un errore di ricezione.

Soluzione:

Questo errore si verifica quando si tenta di accedere a uno degli oggetti specificati mentre sono ancora in corso di caricamento dopo il riavvio di iGateway. Attendere cinque minuti per consentire il completamento dell'operazione e fare clic sui servizi o sugli elementi di gestione desiderati.

Errore di caricamento e importazione durante l'utilizzo di un browser diverso da IE

Sintomo:

Quando si esegue la ricerca di CA Enterprise Log Manager utilizzando Mozilla Firefox, Safari o Chrome, sarà possibile effettuare correttamente multiple attività di CA Enterprise Log Manager. Tuttavia, le attività di caricamento e di importazione verranno interrotte con errori quando si utilizza uno di questi browser. Ecco alcuni esempi:

- L'importazione di una definizione di query verrà interrotta con l'errore "Errore di I/O: Errore di richiesta".
- Il caricamento di un file CSV file con la procedura guidata distribuzione connettori in blocco verrà interrotto nonostante il messaggio"Caricamento file in corso".

Soluzione:

Eseguire la ricerca di CA Enterprise Log Manager con Microsoft Internet Explorer quando si desidera eseguire il caricamento o l'importazione di file.

L'interfaccia utente non viene visualizzata correttamente all'installazione con Remote EEM

Sintomo:

Quando si installa CA Enterprise Log Manager con un server EEM remoto, occasionalmente l'interfaccia utente non viene visualizzata correttamente all'accesso iniziale. L'analisi dei file di registro di iGateway rivela che i servizi agentmanager, calmreporter, subscclient e subscproxy non sono stati avviati.

È possibile visualizzare una sintassi del file di registro simile a questa:

```
[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-msgbroker ] didn't respond OK for the termination
call

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-oaserver ] didn't reaspond OK for the termination
call

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-sapicollector ] didn't reaspond OK for the
termination call

[1087527824] 23/09/09 17:07:46 ERROR :: OutProcessSponsorManager::start :
SponsorGroup [ caelm-java ] failed to start ]

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
agentmanager ] failed to load

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
calmreporter ] failed to load

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscclient ] failed to load

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscproxy ] failed to load
```

Soluzione:

È possibile risolvere questo problema riavviando iGateway ed effettuando nuovamente l'accesso all'interfaccia.

Per riavviare il servizio iGateway:

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Espandere la voce Stato del sistema.
3. Selezionare un server CA Enterprise Log Manager.
4. Fare clic sulla scheda Amministrazione.
5. Fare clic su Riavvia iGateway.

Capitolo 7: Problemi risolti

Questa sezione contiene i seguenti argomenti:

Problemi risolti nella versione r12.1 SP1

In CA Enterprise Log Manager r12.1 SP1 sono stati risolti i seguenti problemi noti riportati dai clienti.

- 18789166-1
- 18790979-1
- 18955095-1
- 18973282-1
- 18982868-1
- 18988854-1
- 19005999-1
- 19066155-1
- 19077668-1
- 19087827-1
- 19127553-1
- 19176852-1
- 19182913-1
- 19188433-2

Capitolo 8: Documentazione

Questa sezione contiene i seguenti argomenti:

Bookshelf

Bookshelf consente di accedere a tutta la documentazione di CA Enterprise Log Manager da una posizione centrale. Bookshelf include:

- Elenco espandibile singolo dei contenuti di tutte le guide in formato HTML
- Ricerca di testo completa in tutte le guide, con termini di ricerca evidenziati nel contenuto e con risultati della ricerca classificati.

  Nota: quando si eseguono ricerche puramente numeriche, inserire un asterisco davanti al valore di ricerca.
- Breadcrumb di collegamento ad argomenti di livello superiore
- Indice singolo valido in tutte le guide
- Collegamenti alle versioni PDF delle guide per la stampa

Modalità di accesso al Bookshelf

I bookshelf di documentazione del prodotto sono disponibili per il download nei file ZIP denominato All Guides Including a Searchable Index (Tutte le Guide con indice di ricerca).

Per accedere al bookshelf di CA Enterprise Log Manager:

1. Andare alla ricerca nella documentazione/nelle guide.
2. Immettere CA Enterprise Log Manager come prodotto, quindi una versione e una lingua e fare clic su Vai.
3. Scaricare il file ZIP sul desktop o in un'altra posizione.
4. Aprire il file ZIP e trascinare la cartella Bookshelf sul desktop o estrarla in un'altra posizione.
5. Aprire la cartella Bookshelf.
6. Aprire il bookshelf:
   - Aprire il file Bookshelf.hta se il bookshelf si trova sul sistema locale e si utilizza Internet Explorer.
   - Aprire il file Bookshelf.html se il bookshelf si trova su un sistema remoto e si utilizza Mozilla Firefox.

   Verrà, quindi, visualizzato il bookshelf.

Appendice A: Marchi di terze parti

Questa sezione contiene i seguenti argomenti:

Adaptive Communication Environment (ACE)

Copyright and Licensing Information for ACE(TM), TAO(TM), and CIAO(TM).

ACE(TM), TAO(TM) and CIAO(TM) are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University Copyright (c) 1993-2003, all rights reserved. Since ACE TAO CIAO are open-source, free software, you are free to use, modify, copy, and distribute--perpetually and irrevocably--the ACE TAO CIAO source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using ACE TAO CIAO.

You can use ACE TAO CIAO in proprietary software and are under no obligation to redistribute any of your source code that is built using ACE TAO CIAO. Note, however, that you may not do anything to the ACE TAO CIAO code, such as copyrighting it yourself or claiming authorship of the ACE TAO CIAO code, that will prevent ACE TAO CIAO from being distributed freely using an open-source development model. You needn't inform anyone that you're using ACE TAO CIAO in your software, though we encourage you to let us know so we can promote your project in the ACE TAO CIAO success stories.

ACE TAO CIAO are provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, ACE TAO CIAO are provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies provide commercial support for ACE and TAO, however. ACE, TAO and CIAO are Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by ACE TAO CIAO or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE, TAO and CIAO web sites are maintained by the Center for Distributed Object Computing of Washington University for the development of open-source software as part of the open-source software community. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the ACE, TAO and CIAO software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source ACE TAO CIAO projects or their designees.

The names ACE(TM), TAO(TM), CIAO(TM), Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE(TM), TAO(TM), or CIAO(TM) nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Software regolati da contratto di licenza Apache

Questo prodotto utilizza il seguente software Apache:

- Ant 1.6.5
- Formatting Objects Processor (FOP) 0.95
- Jakarta POI 3.0
- Log4cplus 1.0.2
- Log4j 1.2.15
- Quartz 1.5.1
- Xerces-C 2.6.0

Portions of this product include software developed by the Apache Software Foundation. Il software Apache viene distribuito in conformità con il seguente contratto di licenza:

Apache License

Version 2,0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

'License' shall mean the terms and conditions for use, reproduction,and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

'Legal Entity' shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, 'control' means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

'You' (or 'Your') shall mean an individual or Legal Entity exercising permissions granted by this License.

'Source' form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

'Object' form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and versions to other media types.

'Work' shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work(an example is provided in the Appendix below).

'Derivative Works' shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

'Contribution' shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, 'submitted' means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as 'Not a Contribution.'

'Contributor' shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) È necessario consegnare agli altri destinatari del Lavoro o Lavoro derivato una copia della presente licenza e

(b) È necessario inserire in ciascun file modificato un avviso evidente che sottolinei la modifica e

(c) È necessario conservare, nel formato Sorgente o qualsiasi Lavoro derivato che venga distribuito, tutti gli avvisi di copyright, brevetto, marchio commerciale e attribuzione del formato Sorgente del Lavoro, esclusi gli avvisi che non riguardano alcuna parte dei lavori derivati e

(d) If the Work includes a 'NOTICE' text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an 'AS IS' BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. Non sussistono circostanze e teorie legali - sia in caso di illecito (incluso negligenza), contratto o altro - a meno che non sia previsto dalla legislazione vigente (ad esempio in caso di negligenza deliberata o evidente) oppure se così è stato concordato in forma scritta - tali da attribuire a un Collaboratore la responsabilità per danni incluso danni diretti, indiretti, speciali, accidentali o consequenziali di qualsivoglia tipo correlati alla presente Licenza oppure causati dall'utilizzo o dall'impossibilità di utilizzare il Lavoro (incluso, ma non solo, i danni per perdita di avviamento, interruzioni dell'attività, guasto del computer o qualsiasi altra perdita o danno commerciale), anche se il Collaboratore era stato informato dalla possibilità di tali danni.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

boost 1.35.0

Questo prodotto include software regolati dal seguente contratto di licenza:

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

JDOM 1.0

Questo prodotto include software sviluppato dal JDOM Project (http://www.jdom.org/). Il software JDOM è distribuito in conformità con il contratto di licenza riportato di seguito.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact .

4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management .

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter and Brett McLaughlin . For more information on the JDOM Project, please see http://www.jdom.org.

PCRE 6.3

Portions of this product include software developed by Philip Hazel. The University of Cambridge Computing Service software is distributed in accordance with the following license agreement.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

End

Zlib 1.2.3

Questo prodotto include zlib, sviluppato da Jean-loup Gailly e Mark Adler.

ZThread 2.3.2

Parti di questo prodotto includono il software sviluppato da Eric Crahen. Il software ZThread viene distribuito in conformità con il seguente contratto di licenza.