CA Enterprise Log Manager

Guida generale

r12.1 SP2

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

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

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

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

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

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

Il produttore di questa Documentazione è CA.

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

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

Riferimenti ai prodotti CA

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.

- Panoramica di avvio rapido: questo argomento esistente è stato aggiornato per fare riferimento a ulteriori tipi di eventi, oltre ai syslog, che possono essere raccolti dall'agente predefinito sul server CA Enterprise Log Manager.
- Avviso di violazione del criterio: questo argomento esistente è stato aggiornato per fare riferimento alla possibilità di inviare avvisi sottoforma di trap SNMP a sistemi di monitoraggio della sicurezza di rete e di impostare gli avvisi per l'esecuzione di un processo IT PAM di output di evento/avviso, ad esempio per creare ticket dell'assistenza tecnica.
- Esplorazione della Bookshelf della documentazione: l'argomento esistente è stato aggiornato per fare riferimento alla nuova Guida alla programmazione tramite API, che ora è visualizzata nella bookshelf di CA Enterprise Log Manager.

Ulteriori informazioni:

Panoramica di avvio rapido (a pagina 15)
Avviso di violazione del criterio (a pagina 57)
Esplorazione della Bookshelf della documentazione (a pagina 67)

Sommario

Capitolo 1: Introduzione

Questa sezione contiene i seguenti argomenti:

Informazioni sulla guida

In questa *Guida generale* viene presentato CA Enterprise Log Manager. Si inizia con rapidi tutorial che consentono sin da subito un'esperienza pratica sul prodotto. Nel primo tutorial viene spiegato come ottenere un sistema CA Enterprise Log Manager a server singolo e come avviare e visualizzare syslog raccolti dai dispositivi UNIX che si trovano molto vicini sulla rete. Nel secondo tutorial vengono illustrati il metodo di installazione di un agente sul sistema operativo Windows, la configurazione di una raccolta registri e la visualizzazione dei registri eventi risultanti. Vengono poi descritte le funzioni principali e cosa consultare per avere ulteriori informazioni. Questa guida è dedicata a tutti i tipi di utente.

Ecco un riassunto dei contenuti:

Sezione	Descrive come
Informazioni su CA Enterprise Log Manager	Integrare CA Enterprise Log Manager nel proprio ambiente di rete corrente.
Distribuzione iniziale rapida	Installare un sistema a server singolo, configurare origini evento syslog, aggiornare il connettore syslog per l'agente predefinito e visualizzare gli eventi perfezionati.
Distribuzione dell'agente Windows	Preparare l'installazione dell'agente, installare un agente per il sistema operativo Windows, configurare un unico connettore per la raccolte basata sugli agenti, aggiornare l'origine evento e visualizzare gli eventi generati.
Funzionalità principali	Trarre vantaggio dalle funzionalità principali, incluse raccolta registri, archivio registri, rapporti e avvisi di conformità.
Ulteriori informazioni su CA Enterprise Log Manager	Ottenere l'informazione desiderata tramite tooltip, guida in linea e bookshelf di documentazione

Nota: per informazioni sul supporto del sistema operativo o sui requisiti di sistema, consultare le *Note della versione*. Per informazioni dettagliate sulle procedure di installazione di CA Enterprise Log Manager e sull'esecuzione di una configurazione iniziale, consultare la *Guida all'implementazione.* Per ulteriori dettagli sull'installazione di un agente, consultare la *Guida all'installazione degli agenti*. Per informazioni sull'utilizzo e la manutenzione del prodotto, consultare la *Guida all'amministrazione.* Per ricevere aiuto per l'utilizzo delle pagine di CA Enterprise Log Manager, consultare la guida in linea.

Informazioni su CA Enterprise Log Manager

CA Enterprise Log Manager è concepito per garantire la conformità e il controllo IT. Consente di raccogliere, normalizzare, aggregare e creare rapporti sull'attività IT e di generare avvisi che richiedano azioni nel caso in cui si verifichino eventuali violazioni di conformità. I dati possono essere raccolti da dispositivi diversi, di sicurezza e non.

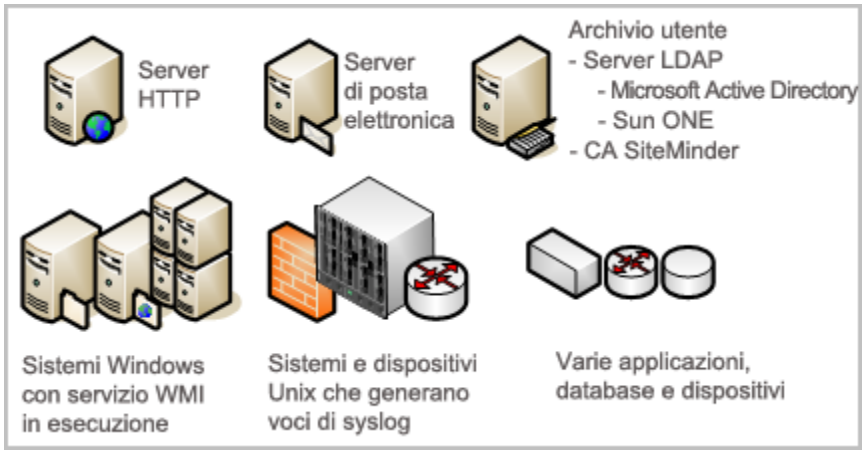
Rete dell'utente-Prima dell'installazione

Le regole e le disposizioni federali impongono la gestione dei record di registro. Per osservarle è necessario:

- Consentire il controllo dei registri.
- Conservare i registri per anni.
- Ripristinare i registri dietro richiesta.

Ciò che rende i record di registro difficili da gestire è il numero elevato, la posizione e la natura temporanea. I registri vengono generati continuamente dall'utente e dalle attività di calcolo del software. La frequenza di generazione viene misurata in eventi al secondo (eps, events per second). Gli eventi non elaborati vengono registrati in ogni sistema attivo, database ed applicazione presente nella rete. In ogni origine evento bisogna eseguire un backup dei record di registro per l'archiviazione prima che essi vengano sovrascritti. È difficile ripristinare i registri evento quando i backup di diverse origini eventi vengono memorizzati separatamente.

Ciò che rende noioso interpretare gli eventi non elaborati è il loro formato di stringa, in cui la gravità di evento non viene messa in risalto. Inoltre, dati analoghi ma di diversi sistemi possono differire fra loro.



L'efficienza operativa richiede una soluzione in grado di consolidare tutti i registri, di renderli semplici da leggere, di automatizzare l'archiviazione e di semplificarne il ripristino. CA Enterprise Log Manager offre questi vantaggi e, in caso di eventi critici, consente di inviare avvisi a singole persone ed a sistemi.

Elementi da installare

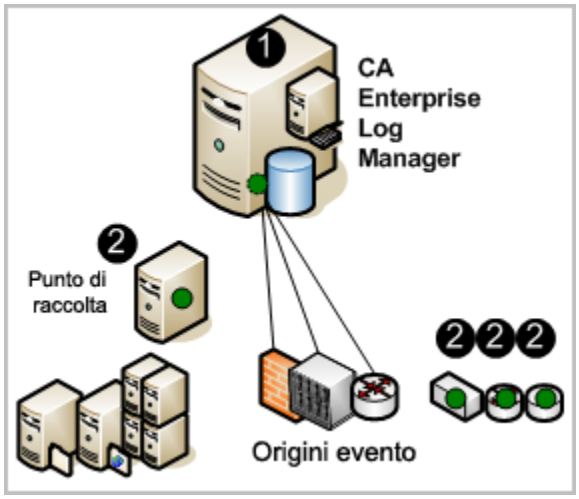
Non occorre molto tempo per configurare una soluzione a server singolo e iniziare a raccogliere eventi.

I dischi di installazione includono i seguenti componenti:

- Sistema operativo (Red Hat Enterprise Linux) per l'applicazione software
- Server CA Enterprise Log Manager
- Agente CA Enterprise Log Manager (di seguito ci si riferisce ad esso come "agente")

Nella figura seguente, CA Enterprise Log Manager viene raffigurato come un server contenente un piccolo server, un cerchio scuro (verde) e un database. Il piccolo server rappresenta il repository locale che archivia il contenuto a livello di applicazione. Il cerchio scuro rappresenta l'agente predefinito, mentre il database indica l'archivio registro eventi in cui i registri eventi in ingresso vengono elaborati e resi disponibili per query e rapporti.

I cerchi scuri (verdi) sul punto di raccolta e sulle altre origini evento rappresentano gli agenti installati separatamente. L'installazione degli agenti è facoltativa. È possibile raccogliere syslog da origini evento compatibili con UNIX tramite l'agente predefinito dopo aver completato la configurazione richiesta.



I numeri nella figura si riferiscono a questi passaggi:

1. Installare il sistema operativo per l'applicazione software e quindi installare l'applicazione CA Enterprise Log Manager. Non appena le origini vengono configurate per l'invio dei syslog a CA Enterprise Log Manager e si indicano le destinazioni syslog nella configurazione del connettore dell'agente predefinito, i syslog vengono raccolti e perfezionati per semplificarne l'interpretazione.
2. (Facoltativo) È possibile installare un agente su un host dedicato come punto di raccolta, oppure è possibile installare gli agenti direttamente sugli host con le origini che generano gli eventi che si desidera raccogliere.

Nota: per informazioni sull'installazione dell'applicazione software, consultare la *Guida all'implementazione*. Per informazioni sull'installazione degli agenti, consultare la *Guida all'installazione degli agenti*.

Ulteriori informazioni:

Installare un agente (a pagina 39)

Capitolo 2: Distribuzione iniziale rapida

Questa sezione contiene i seguenti argomenti:

Panoramica di avvio rapido

È possibile ottenere una distribuzione semplice e funzionante di CA Enterprise Log Manager con un dispositivo software. Il connettore syslog predefinito consente all'agente predefinito di ricevere gli eventi di syslog generati. È sufficiente configurare le origini di syslog per inviare gli eventi di syslog a CA Enterprise Log Manager e modificare la configurazione del connettore di syslog per identificare le destinazioni di syslog. Ciò che si riceve dipende dalla larghezza di banda e dalla latenza tra le origini del server e di syslog.

I sensori di registro, inclusi WinRM e ODBC, supportano la raccolta diretta dei registri da oltre venti origini di eventi diverse da syslog. Il sensore di registro WinRM permette di raccogliere gli eventi direttamente dai server con sistemi operativi Windows, come Forefront Security for Exchange Server, Forefront Security for SharePoint Server, Microsoft Office Communication Server e il server e i servizi virtuali di Hyper-V come i Servizi certificati Active Directory. Il sensore di registro ODBC permette di acquisire gli eventi generati dai database di Oracle9i o SQL Server 2005. Per ulteriori informazioni, consultare Matrice di integrazione del prodotto CA Enterprise Log Manager.

Per installare CA Enterprise Log Manager sono necessarie le credenziali EiamAdmin. Come utente con privilegi avanzati EiamAdmin, si configura un account di Amministratore da utilizzare per eseguire la configurazione. Se si accede con le credenziali di amministratore, è possibile verificare che la configurazione sia funzionante visualizzando gli eventi di automonitoraggio.

Installazione di un sistema a server singolo.

La distribuzione più semplice che permette di visualizzare gli eventi interrogati è un sistema a server singolo. Assicurarsi di selezionare una macchina con caratteristiche pari o superiori ai requisiti hardware minimi per un dispositivo software CA Enterprise Log Manager.

Nota: consultare le *Note di rilascio* per l'elenco degli hardware certificati, il supporto del sistema operativo e i requisiti del software del sistema e di servizio.

Per installare un CA Enterprise Log Manager per un sistema a server singolo

1. Avere a portata di mano le seguenti informazioni:
   - Una password da utilizzare come password root
   - Nome host per la propria applicazione
   - Se non si utilizza DHCP, indirizzo IP statico, subnet mask e gateway predefinito del dispositivo
   - Dominio dell'applicazione

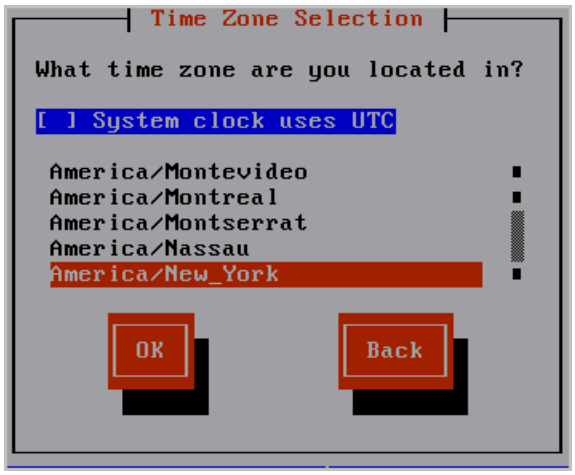
     Nota: il dominio deve essere registrato con i server DNS sulla propria rete per completare l'installazione.
   - Indirizzi IP dei server DNS
   - (Facoltativo) Indirizzo IP del server con orario NTP
   - Una password per il nome del super utente per l'installazione predefinito, EiamAdmin
   - CAELM.

     È il nome dell'applicazione predefinita per l'applicazione CA Enterprise Log Manager.

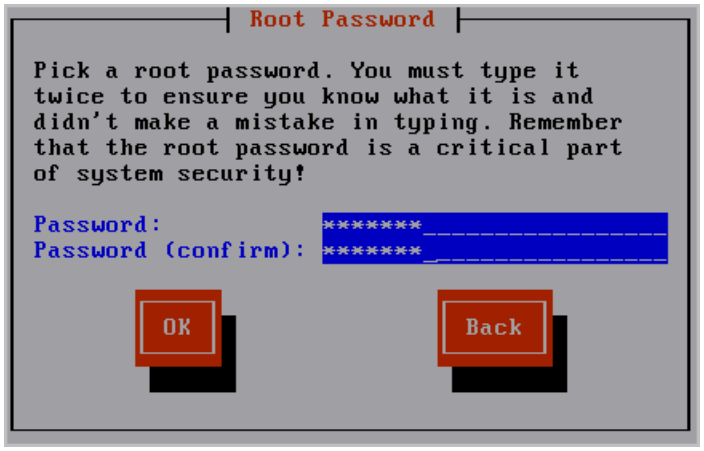
2. Installare il sistema operativo preconfigurato utilizzando il supporto creato per il pacchetto di download di CA Enterprise Log Manager. Durante l'installazione del sistema operativo, eseguire le seguenti procedure:

   a. Scegliere un tipo di tastiera. Quella predefinita è U.S.

   b. Scegliere un fuso orario, ad esempio America/New York, e selezionare OK.



   c. Digitare la password da utilizzare come password root, quindi digitarla nuovamente per conferma. Scegliere OK.



Verranno visualizzate le informazioni di avanzamento dell'installazione.

d. Rimuovere il disco di installazione del sistema operativo e premere Invio per riavviare il sistema.

Il sistema si riavvia ed accede alla configurazione non interattiva. Verranno visualizzati messaggi che descrivono l'avanzamento dell'installazione. Le informazioni dettagliate su questa installazione vengono salvate nel file /tmp/pre-install_ca-elm.log.

Verrà visualizzato il seguente prompt:

```
Inserire il disco di installazione dell'applicazione CA Enterprise Log
Manager r12 e premere Invio.
```

3. Inserire il disco dell'applicazione CA Enterprise Log Manager. Premere Invio.

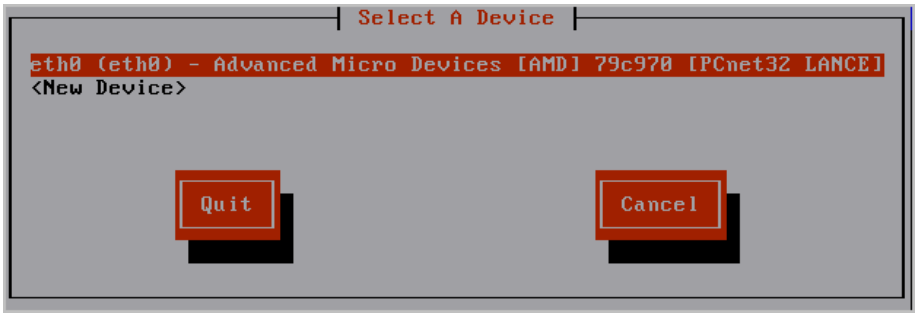
   Il sistema viene riesaminato per vedere se soddisfa le specifiche minime consigliate per ottenere prestazioni ottimali. In caso contrario, viene visualizzato un prompt che chiede se si desidera interrompere il processo di installazione.

   Verrà visualizzato il seguente prompt:

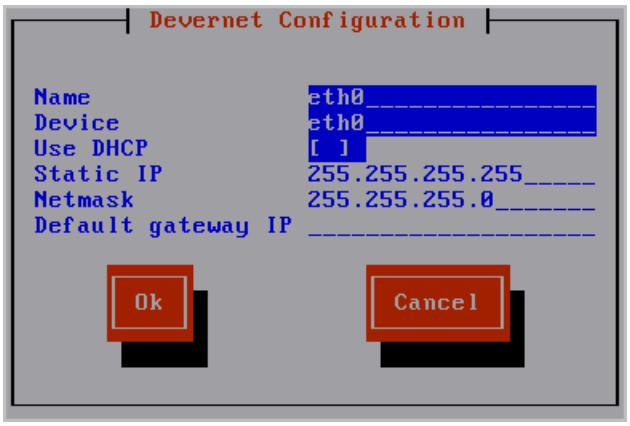
```
Immettere un nuovo nome host:
```

4. Immettere il nome host per questa applicazione software CA Enterprise Log Manager. Ad esempio, immettere CALM1.

5. Accettare il dispositivo predefinito, eth0. Premere Invio per passare alla schermata successiva.



6. Eseguire una delle seguenti operazioni e selezionare OK.
   - Selezionare Usa DHCP, un'opzione accettabile solo per un sistema di verifica indipendente.
   - Immettere indirizzo IP statico, subnet mask e indirizzo IP del gateway predefinito da associare al nome host inserito.



   I servizi di rete vengono riavviati con le nuove impostazioni, che vengono visualizzate.

   Viene visualizzato il seguente messaggio:

   ```
   Modificare la configurazione di rete? (n):
   ```

7. Esaminare le impostazioni di rete. Se soddisfacenti, digitare n o premere Invio quando viene visualizzato il messaggio che permette di modificare le impostazioni di rete.

   Viene visualizzato il seguente messaggio:

   ```
   Immettere il nome di dominio per questo sistema:
   ```

8. Immettere il nome di dominio, come <aziendapersonale>.com.

   Viene visualizzato il seguente messaggio:

   ```
   Inserire un elenco di server DNS da utilizzare separati da virgola:
   ```

9. Immettere gli indirizzi IP dei server DNS interni separati da virgole senza spazi.

   La data e l'ora del sistema vengono visualizzate con il seguente messaggio:

   ```
   Modificare la data e l'ora del sistema? (n)
   ```

10. Riesaminare la data e l'ora del sistema visualizzate. Se soddisfatti, digitare n oppure premere Invio.

    Viene visualizzato il seguente messaggio:

    ```
    Configurare il sistema per aggiornare l'ora attraverso NTP?
    ```

11. Se si desidera utilizzare un server Network Time Protocol (NTP), procedere come indicato di seguito. In caso contrario, specificare no e andare al passaggio successivo.

    a. Rispondere sì al messaggio.

       Se si specifica sì, viene visualizzato il seguente messaggio:

       ```
       Immettere il nome del server NTP oppure l'indirizzo IP
       ```

    b. Immettere il nome host o l'indirizzo IP del server NTP.

       Verrà visualizzato un messaggio di conferma simile al seguente: "Il sistema è stato configurato per aggiornare l'ora a mezzanotte utilizzando il server NTP che si trova in <serverntp>."

12. Leggere i contratti di licenza con l'utente finale (EULA) presentati e rispondere come segue:

    a. Leggere l'EULA di Java Development Kit (JDK) di Sun.

       Al termine dell'EULA, viene visualizzato il seguente messaggio:

       ```
       Accettare i termini della licenza sopracitati? [sì o no]
       ```

    b. Digitare sì se si accettano i termini.

       Le informazioni sulla registrazione del prodotto vengono visualizzate seguite da questo messaggio:

       ```
       Premere Invio per continuare.
       ```

    c. Premere Invio.

       I messaggi indicano che in preparazione dell'installazione di CA Enterprise Log Manager vengono configurate le impostazioni del sistema. Viene visualizzato il contratto di licenza per l'utente finale CA.

    d. Leggere il contratto CA EULA.

       Al termine della licenza, viene visualizzato il seguente messaggio:

       ```
       Accettare i termini della licenza sopracitati? [Sì o no]:
       ```

    e. Digitare sì se si accettano i termini.

       Vengono visualizzate le informazioni sul server CA EEM.

13. Rispondere ai seguenti prompt per configurare CA EEM.

    ```
    Utilizzare un server EEM locale o remoto?
    Immettere l (locale) o r (remoto):
    ```

    a. Per creare un sistema di verifica indipendente, immettere l per locale.

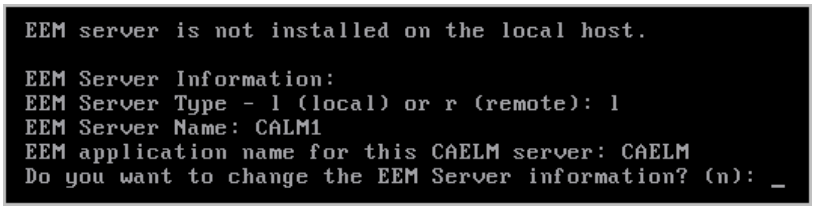
       ```
       Immettere la password per l'utente EiamAdmin del server EEM:
       Confermare la password per l'utente EiamAdmin del server EEM:
       ```

b. Digitare la password da assegnare all'utente EiamAdmin con privilegi avanzati predefinito, quindi digitarla nuovamente.

```
Immettere il nome di un'applicazione per questo server CAELM (CAELM):
```

c. Premere Invio per accettare CAELM, il nome predefinito dell'applicazione per CA Enterprise Log Manager.

Le informazioni sul server EEM inserite finora vengono visualizzate con un messaggio che chiede se si desidera effettuare modifiche.



d. Premere Invio o digitare n per accettare le informazioni sul server CA EEM inserite.

Il processo di installazione ha inizio. Vengono visualizzati messaggi che mostrano l'avanzamento man mano che viene installato ogni componente di CA Enterprise Log Manager, che le registrazioni vengono completate, che i certificati vengono acquisiti, che i file vengono importati e i componenti configurati. Viene visualizzato il messaggio Installazione di CA ELM riuscita. Al termine dell'installazione, il sistema visualizza l'indirizzo di accesso alla console.

14. Rispondere al seguente prompt:

```
Do you want to run CAELM Server in FIPS mode?
Digitare Yes o No.
```

Se si immette y, il server CA Enterprise Log Manager verrà avviato in modalità FIPS. Se si immette n, verrà avviato in modalità Non FIPS.

15. Prendere nota di questo indirizzo. Si tratta dell'indirizzo che si immette in un browser per accedere a questo server CA Enterprise Log Manager. Ovvero, https://<hostname>:5250/spin/calm.

Viene visualizzato un prompt di accesso <nomehost>. È possibile ignorarlo.

Nota: se per qualsiasi motivo si desidera visualizzare il prompt del sistema operativo da questo prompt di accesso, è possibile farlo digitando caelmadmin e la password predefinita, ovvero la password assegnata all'account utente EiamAdmin. Si utilizza l'account caelmadmin per accedere al dispositivo sulla console o attraverso SSH.

16. Proseguire come indicato di seguito:
    - Se si è configurato un indirizzo IP statico, assicurarsi di registrarlo con i server DNS specificati al passaggio 9.
    - Se è stato configurato DHCP, aggiornare i file degli host sulla macchina da cui si intende esplorare questo server.
    - Passare all'URL di cui si è preso nota nel passaggio 14 e configurare il primo Amministratore.

Aggiornare il file hosts Windows

Durante l'installazione di CA Enterprise Log Manager, è possibile identificare uno o più server DNS oppure selezionare Usa DHCP. Se si è selezionato DHCP, è necessario aggiornare il file hosts di Windows sul computer da cui si è previsto di accedere a CA Enterprise Log Manager con il proprio browser.

Per aggiornare il file hosts sull'host con il proprio browser

1. Aprire Esplora risorse e passare a C:\WINDOWS\system32\drivers\etc.
2. Aprire il file hosts con un editor, ad esempio Blocco note.
3. Aggiungere una voce con l'indirizzo IP del server CA Enterprise Log Manager e il corrispondente nome host.
4. Selezionare Salva dal menu File, quindi chiudere il file.

Configurare il primo amministratore

Dopo aver installato un sistema a server singolo CA Enterprise Log Manager, predisporre la configurazione andando all'URL di CA Enterprise Log Manager da una workstation remota. Quindi accedere e creare un account amministratore che è possibile utilizzare per eseguire la configurazione.

Nota: allo scopo di questa distribuzione iniziale rapida, verranno utilizzati l'archivio utenti predefinito e i criteri delle password predefiniti. Di solito, essi vengono configurati prima di aggiungere il primo amministratore.

Per configurare il primo amministratore

1. Eseguire la connessione al seguente URL dal proprio browser: per nomehost si intende il nome host o l'indirizzo IP del server su cui è stato installato CA Enterprise Log Manager.

   `https://<nomehost>:5250/spin/calm`

2. Se viene visualizzato un avviso di protezione, comportarsi come di seguito descritto:

   a. Fare clic su Visualizza certificato.

   b. Fare clic su Installa certificato, accettare i valori predefiniti e terminare la procedura guidata di importazione.

      Viene visualizzato un avviso di protezione che afferma che si sta per installare un certificato che indica di rappresentare il nome host del server CA Enterprise Log Manager.

   c. Fare clic su Sì.

      Il certificato radice viene installato e un messaggio informa del corretto completamento dell'importazione.

   d. Fare clic su OK.

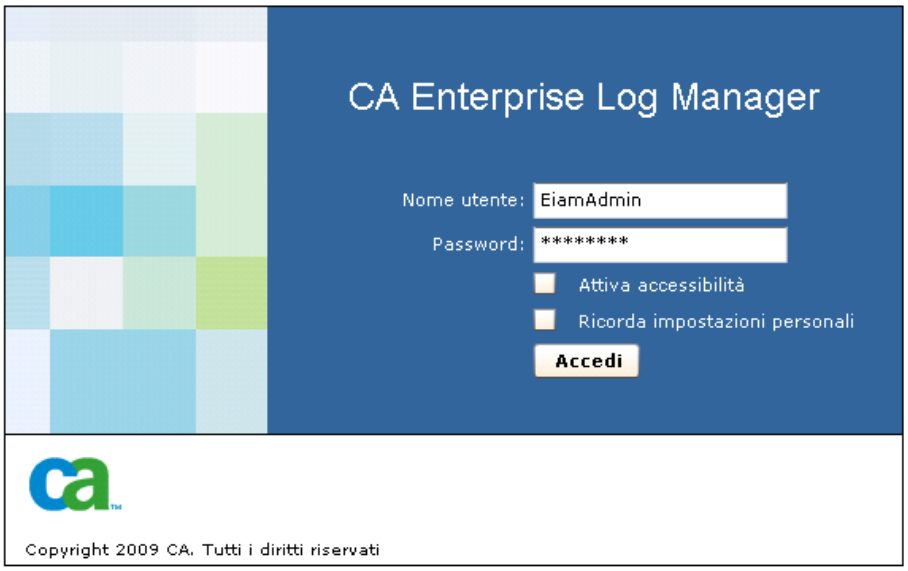
      Viene visualizzata la finestra di dialogo Certificati attendibili.

   e. (Facoltativo) Fare clic sul Percorso certificazione e verificare che lo stato del certificato sia OK.

   f. Fare clic su OK, quindi su Sì.

      Viene visualizzata la pagina di accesso.

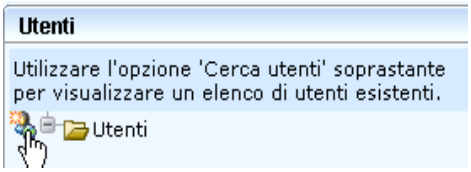
3. Accedere con il nome utente EiamAdmin e la password creata al momento dell'installazione del software. Fare clic su Accedi.



L'applicazione consente di visualizzare soltanto la scheda Amministrazione e la sottoscheda Gestione utenti e accessi come attive.

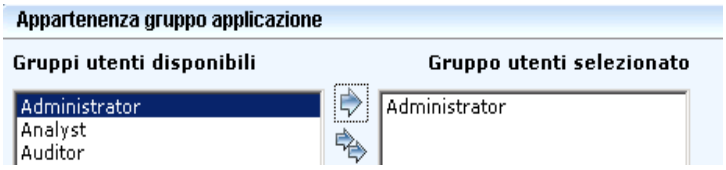
4. Fare clic su Utenti.

5. Fare clic su Aggiungi nuovo utente.

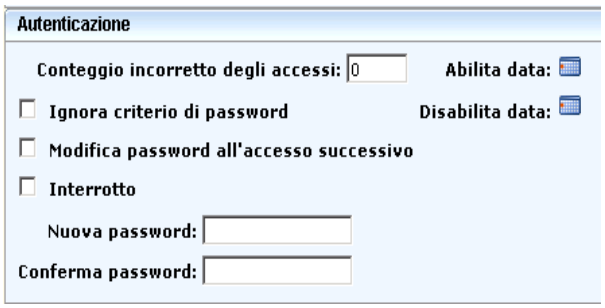


6. Inserire il proprio nome nel campo Nome e fare clic su Aggiungi dettagli utente applicazione.

7. Selezionare l'amministratore e spostarlo nell'elenco Gruppi utente selezionati.



8. In Autenticazione, inserire una password per il nuovo account nei due campi di inserimento e conferma.



9. Fare clic su Salva, quindi su Chiudi. Fare clic su Chiudi.
10. Fare clic sul link di disconnessione posizionato sulla barra degli strumenti.

    Viene visualizzata la pagina di accesso.

11. Accedere nuovamente a CA Enterprise Log Manager con le credenziali di amministratore appena definite.

    CA Enterprise Log Manager viene aperto con tutte le funzionalità abilitate. Vengono visualizzate la scheda Query e rapporti e la sottoscheda Query.

12. (Facoltativo) Visualizzare i tentativi di accesso come segue:

    a. Selezionare l'accesso al sistema dall'elenco di tag delle query.

    b. Selezionare dall'elenco delle query Dettagli accesso di sistema.

    I risultati delle query mostrano due tentativi di accesso, prima come EiamAdmin, quindi con il nome amministratore (i tentativi sono contrassegnati da una S che sta per "successfull", vale a dire riuscito).

Livello di gravità CA	Data	Account	Esecutore	Host	Nome registro	Categoria	Azione	Risultato
Informazioni	Giovedì 12/11/2009 16:07:52	admin	admin	ca-elm	CALM	System Access	Login Attempt	S
Informazioni	Giovedì 12/11/2009 16:09:28	liuyue	liuyue	ca-elm	CALM	System Access	Login Attempt	S
Informazioni	Giovedì 12/11/2009 16:16:11	admin	admin	ca-elm	CALM	System Access	Login Attempt	S
Informazioni	Giovedì 12/11/2009 16:17:17	song11	song11	ca-elm	CALM	System Access	Login Attempt	S

Configurare le origini evento Syslog

Per attivare la raccolta diretta degli eventi syslog da parte dell'agente predefinito esistente in ogni server CA Enterprise Log Manager, iniziare identificando le origini dell'evento syslog da cui si desidera raccogliere gli eventi e determinando l'integrazione associata. Quindi eseguire le due azioni seguenti in qualsiasi ordine.

- Configurare le origini evento syslog. Accedere a ogni host su cui viene eseguita un'origine evento syslog e configurarlo come riportato nella guida al connettore per quell'integrazione syslog.
- Configurare il connettore syslog sull'agente predefinito per aggiungere le integrazioni syslog di destinazione associate alle origini evento configurate.

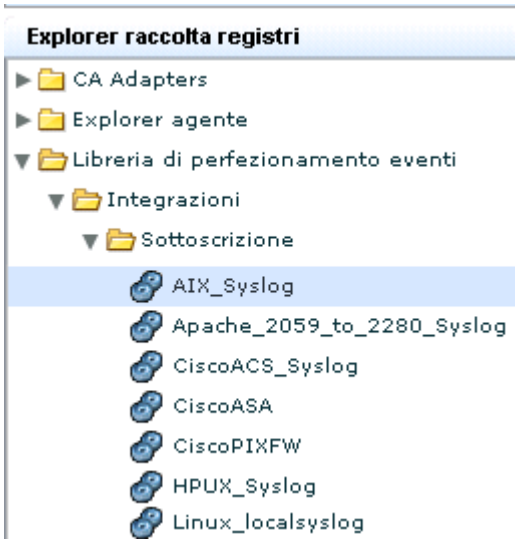
Al termine dei due passaggi della configurazione, hanno inizio la raccolta eventi e il perfezionamento. Quindi, è possibile utilizzare CA Enterprise Log Manager per visualizzare o creare un rapporto sugli eventi di cui ci si occupa in un formato standardizzato. È inoltre possibile generare avvisi durante l'esecuzione di eventi specifici.

Configurare l'origine di un evento syslog selezionato

1. Accedere all'host con un'origine evento syslog di destinazione.
2. Avviare CA Enterprise Log Manager da un browser in questo host.
3. Fare clic sulla scheda Amministrazione e sulla sottoscheda Raccolta registri.

   Viene visualizzato Explorer raccolta registri.
4. Espandere Libreria di perfezionamento eventi, Integrazioni e Sottoscrizione.

   Viene visualizzato l'elenco delle integrazioni predefinite. Di seguito un semplice esempio:



5. Selezionare l'integrazione per l'origine evento da configurare. Ad esempio, se si desidera raccogliere i syslog generati da un sistema operativo AIX, si dovrà selezionare AIX_Syslog.

   Vengono visualizzati i dettagli dell'integrazione.

6. Fare clic sul pulsante Aiuto posizionato proprio sopra il nome dell'integrazione nel pannello a destra.

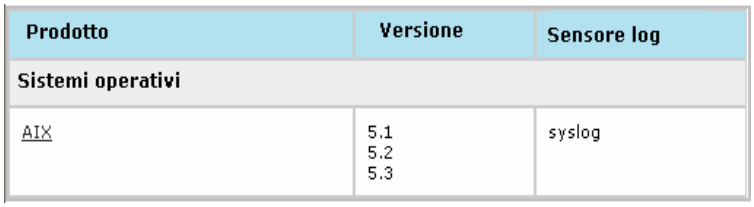
   Viene visualizzata la guida al connettore per l'integrazione selezionata.

7. Fare clic sulla sezione nei requisiti di configurazione dell'origine evento. In questo esempio, la documentazione descrive come eseguire la configurazione dell'origine evento del sistema operativo AIX per inviare i relativi syslog a CA Enterprise Log Manager.

Esempio - Fonte alternativa per le Guide al connettore: supporto online

È possibile aprire una guida al connettore selezionata dall'interno dell'interfaccia utente CA Enterprise Log Manager o dal supporto online CA. Di seguito viene presentato un esempio che mostra come aprire una guida al connettore da questa fonte alternativa.

1. Accedere al supporto online CA.
2. Selezionare CA Enterprise Log Manager dall'elenco a discesa della pagina Seleziona un prodotto.
3. Scorrere fino a Stato prodotto e selezionare la matrice di certificazione CA Enterprise Log Manager.
4. Selezionare Matrice integrazione prodotto.
5. Trovare la categoria per l'integrazione associata all'origine evento che si sta configurando. Ad esempio, se l'origine evento è il sistema operativo AIX, scorrere fino alla categoria Sistemi operativi e fare clic sul link AIX.



Prodotto	Versione	Sensore log
Sistemi operativi		
AIX	5.1 5.2 5.3	syslog

Modificare il connettore syslog

Ogni CA Enterprise Log Manager dispone di un agente predefinito. Quando si installa un CA Enterprise Log Manager , l'agente predefinito dispone di un connettore parzialmente configurato chiamato Syslog_Connector basato sul listener, Syslog. Questo listener riceve eventi syslog grezzi sulle porte predefinite non appena si configurano le origini evento per inviare syslog a CA Enterprise Log Manager. Tuttavia, perché CA Enterprise Log Manager possa perfezionare questi eventi grezzi, occorre modificare Syslog_Connector. Alcune modifiche sono obbligatorie, altre facoltative.

- È necessario identificare le destinazioni syslog quando si modifica questo connettore. Selezionare come destinazione syslog ogni integrazione che corrisponda a una o più origini evento già configurate o che si prevede di configurare. Identificare destinazioni syslog consente a CA Enterprise Log Manager di perfezionare correttamente gli eventi.
- Se lo si desidera, è possibile applicare regole di soppressione, limitare l'accettazione dei syslog a host attendibili, specificare porte di attesa diverse dalla 514, la famosa porta UDP syslog, e dalla 1468, la porta TCP predefinita e/o aggiungere nuovi fusi orari per gli host attendibili.

Per modificare il connettore syslog per un agente predefinito

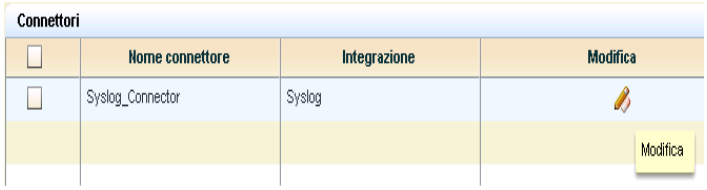
1. Fare clic sulla scheda Amministrazione.

   Verrà visualizzata la sottoscheda Raccolta registri.

2. Espandere l'Explorer agente e poi il Gruppo agenti predefinito o il gruppo definito dall'utente al momento della configurazione di CA Enterprise Log Manager.

3. Selezionare il nome di un server CA Enterprise Log Manager.

   Verrà visualizzato il connettore Syslog_Connector.



4. Fare clic su Modifica.

   La modifica guidata del connettore viene visualizzata con selezionato il passaggio relativo ai dettagli connettore.

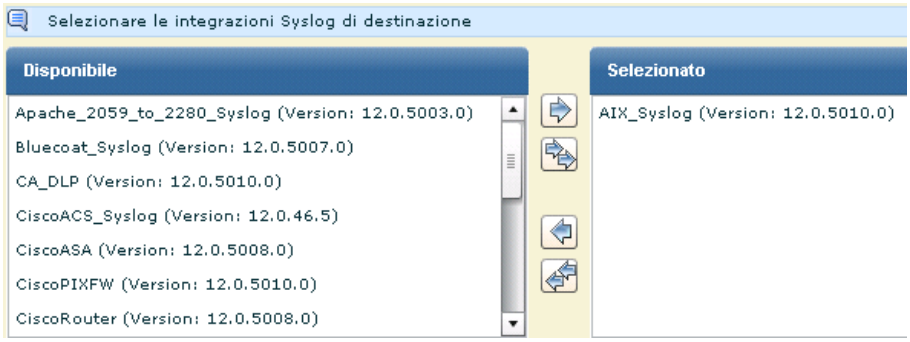
5. (Facoltativo) Fare clic su Applica regole di soppressione. Se si desidera sopprimere, ovvero *non* raccogliere, un evento syslog qualunque, spostare il tipo di evento dall'elenco disponibile a quello selezionato. Selezionare l'evento da spostare e fare clic sul pulsante corrispondente all'azione.

6. Fare clic sul passaggio Configurazione connettore.

   Tutte le integrazioni disponibili sono selezionate per impostazione predefinita.

7. Selezionare le destinazioni syslog spostando le integrazioni syslog verso la destinazione dall'elenco disponibile a quello selezionato.

   Ad esempio, se il sistema operativo AIX è stato configurato su un host della propria rete, sarà necessario spostare la destinazione syslog, AIX_Syslog, dall'elenco disponibile all'elenco selezionato.



8. (Facoltativo) Identificare gli host attendibili dai quali il connettore syslog accetterà gli eventi in ingresso. Immettere l'indirizzo IP nel campo, quindi fare clic su Aggiungi. Ripetere l'operazione per tutti gli host attendibili. Successivamente, quando un evento viene ricevuto da un host non configurato come attendibile, tale evento verrà respinto.

   Nota: è buona abitudine configurare gli host attendibili. Di solito vengono configurati tutti gli host sui quali sono state configurate origini evento per l'invio di syslog a CA Enterprise Log Manager. Specificare gli host attendibili assicura che l'agente predefinito non accetti eventi dai rogue system configurati dall'autore di un attacco per inviare eventi al listener di syslog.

9. (Facoltativo) Aggiungere porte.

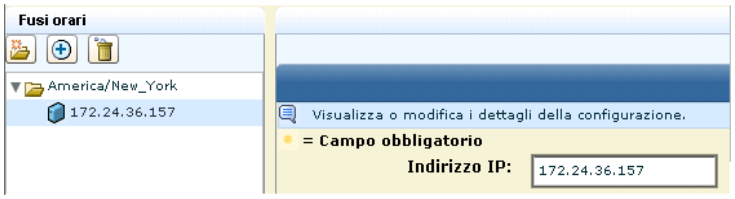
   Generalmente, è possibile accettare le porte UPD e TCP predefinite per l'agente predefinito.

   Nota: è possibile ottenere prestazioni superiori definendo un connettore syslog per diversi tipi di evento e specificando porte diverse per ognuno di essi. Assicurarsi di selezionare porte non utilizzate quando si eseguono nuove assegnazioni di porte.

10. (Facoltativo) Aggiungere un fuso orario solo se si raccolgono syslog da computer in fusi orari diversi dall'applicazione software.

    a. Fare clic su Crea cartella ed espandere la cartella.

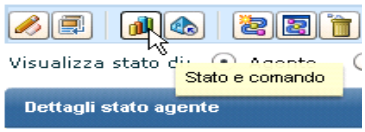
    b. Selezionare la voce vuota sotto la cartella. Inserire l'indirizzo IP di un host attendibile configurato per questo connettore o del server di riferimento orario NTP specificato al momento dell'installazione del CA Enterprise Log Manager.



11. Fare clic su Salva e chiudi.

12. Visualizzare lo stato.

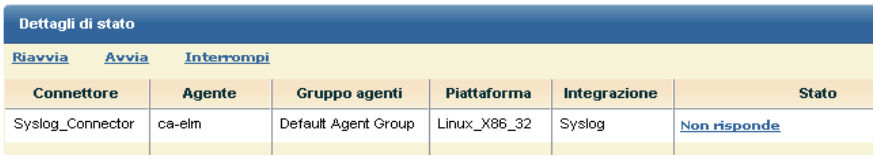
    a. Fare clic su Stato e comando.



    L'opzione Visualizza stato degli agenti è selezionata. Il nome host del server installato verrà visualizzato nella colonna Agente, dato che l'agente predefinito si trova su questo server. Lo stato mostrato è quello di funzionamento.

    b. Fare clic sul link In esecuzione per visualizzare i dettagli.

    c. Fare clic sul pulsante Connettori per visualizzare lo stato dei connettori.



d. Fare clic sul link In esecuzione.

Verranno visualizzati CPU in percentuale, utilizzo della memoria, media di eventi al secondo (EPS) e conteggio eventi filtrati.

Visualizzare eventi Syslog

Uno dei modi più veloci per visualizzare i risultati delle query sugli eventi raccolti da un listener di syslog consiste nell'utilizzo del prompt per host.

Per visualizzare gli eventi syslog

1. Selezionare la scheda Query e rapporti.

   Viene visualizzata la sottoscheda Query.

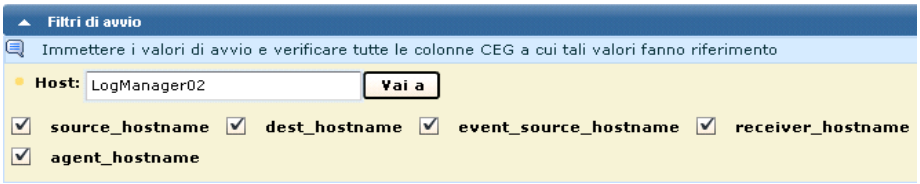
2. Espandere i prompt sotto Elenco Query e selezionare Host.

3. Inviare una query per gli eventi raccolti dall'agente predefinito.

   a. Immettere il nome host dell'agente predefinito nel campo Host, che corrisponde al nome del CA Enterprise Log Manager su cui esso risiede.

   b. Selezionare agent_hostname.

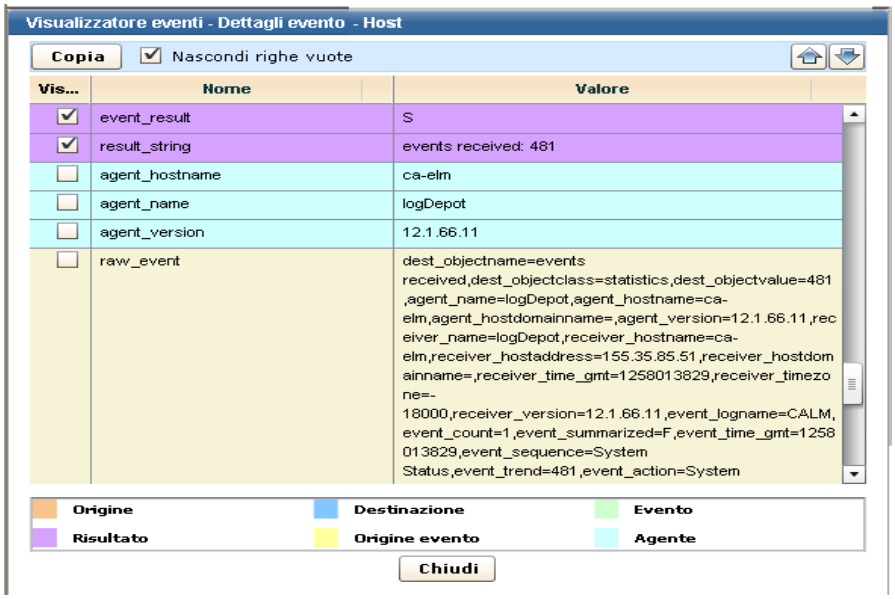
   c. Fare clic su Vai a.



4. Visualizzare i risultati da esaminare.
   a. Fare clic sulla colonna Risultati per ordinare in base ai risultati.
   b. Scorrere al primo risultato di E di Errore. Si supponga che si tratti di un avviso di configurazione nella categoria Gestione configurazione.
   c. Fare doppio clic per selezionare la riga da visualizzare in dettaglio.

   Verrà visualizzato il Visualizzatore eventi.

5. Scorrere fino all'area in cui è visualizzato il Risultato. Nell'esempio, l'errore è un avviso che indica la necessità di configurare il modulo di sottoscrizione. Si tratta di un avviso da ignorare fino al termine dell'installazione di tutti i server CA Enterprise Log Manager pianificati.



Capitolo 3: Distribuzione dell'agente Windows

Questa sezione contiene i seguenti argomenti:

Creare un account utente per l'agente

Prima di installare un agente su un sistema operativo Windows, creare un nuovo account per l'agente nella cartella utenti di Windows. Lo scopo della creazione di questo account con pochi privilegi è consentire all'agente di essere utilizzato con la minor quantità possibile di privilegi. Quando si installa l'agente, si forniscono il nome utente e la password creati qui.

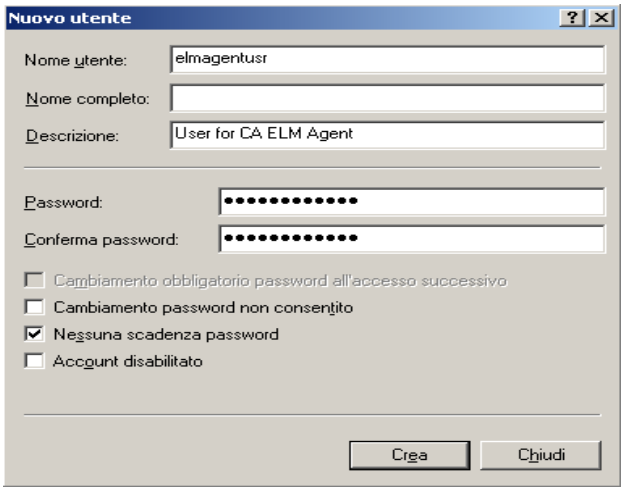
Nota: è possibile saltare questo passaggio e specificare le credenziali di dominio di un Amministratore per l'agente nel momento in cui si esegue l'installazione, ma non è considerata una buona prassi.

Per creare un account utente Windows per l'agente

1. Effettuare l'accesso all'host in cui si prevede di installare l'agente. Utilizzare le credenziali di amministratore.
2. Fare clic su Start, Programmi, Strumenti di amministrazione, Gestione computer.
3. Espandere Utenti e gruppi locali.
4. Fare clic con il tasto destro su Utenti e selezionare Nuovo utente.

   Viene visualizzata la finestra di dialogo Nuovo utente di Windows.
5. Immettere un nome utente e immettere due volte una password. Una password efficace è composta da una combinazione di lettere, numeri e caratteri speciali. Ad esempio, calmr12_agent. Se lo si desidera, immettere una descrizione.

   Importante: Ricordare questo nome e questa password oppure registrarli. Sarà necessario inserirli al momento dell'installazione dell'agente.



6. Fare clic su Crea. Fare clic su Chiudi.

Ulteriori informazioni:

Installare un agente (a pagina 39)

Impostare la chiave di autenticazione agente.

Prima di installare il primo agente, occorre conoscere la chiave di autenticazione agente. Se nessuna chiave è stata impostata, è possibile utilizzare quella predefinita. Se una chiave è già stata impostata, utilizzare quella corrente, oppure impostarne una nuova. La chiave di autenticazione agente qui configurata deve essere inserita durante l'installazione di ogni agente. Soltanto un amministratore può eseguire questa attività.

Per impostare la chiave di autenticazione agente

1. Aprire il browser sull'host in cui si prevede di installare l'agente ed inserire l'URL del server CA Enterprise Log Manager per questo agente. Di seguito un esempio:

   `https://<indirizzo IP>:5250/spin/calm/`

2. Accedere al server CA Enterprise Log Manager. Immettere il nome utente e la password, quindi fare clic su Accedi.
3. Fare clic sulla scheda Amministrazione.

   Nel pannello di sinistra viene visualizzato Explorer raccolta registri.

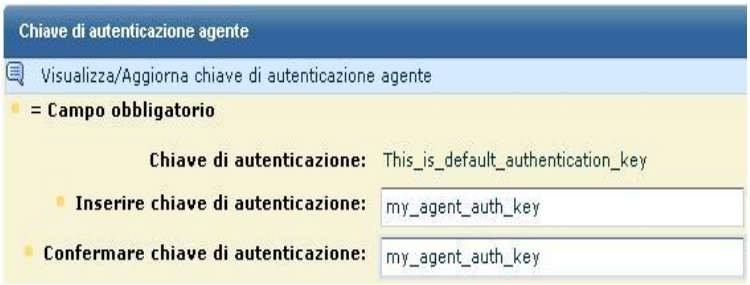
4. Selezionare la cartella Explorer agente.

   Nel pannello principale verrà visualizzata una barra degli strumenti.

5. Fare clic su Chiave di autenticazione agente.

6. Immettere la chiave di autenticazione agente da utilizzare per l'installazione dell'agente o prendere nota della voce corrente.

   Importante: Ricordare o registrare questa chiave. Sarà necessaria per installare l'agente.



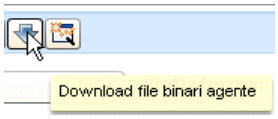
7. Fare clic su Salva.
8. Proseguire con il passaggio successivo, Download del programma di installazione dell'agente.

Download del programma di installazione dell'agente

Se è stata impostata la chiave di autenticazione dell'agente, è possibile scaricare il programma di installazione dell'agente sul desktop.

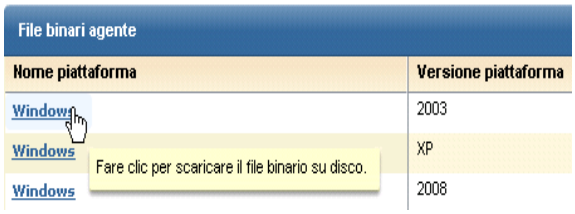
Per scaricare il programma di installazione dell'agente

1. Fare clic su Download file binari agente dalla barra degli strumenti visualizzata per Explorer agente.



   I link per i file binari agente disponibili vengono visualizzati sul pannello principale.

2. Fare clic sul link di Windows per installare l'agente su un server dotato di sistema operativo Windows Server 2003.



Viene visualizzata la finestra di dialogo Seleziona posizione per il download in base a <indirizzo IP>.

3. Selezionare il desktop e fare clic su Salva.

Viene visualizzato un messaggio che mostra l'avanzamento del download del file binario dell'agente selezionato, seguito da un messaggio di conferma.

4. Fare clic su OK.
5. Ridurre a icona il browser ma lasciare aperta la connessione, in modo che sia possibile verificare rapidamente l'installazione dopo il completamento.

   L'utilità di avvio della configurazione dell'agente viene visualizzata sul desktop.

Installare un agente

Prima di iniziare, è necessario disporre di quanto segue:

- Indirizzo IP del server CA Enterprise Log Manager dal quale è stato scaricato il programma dell'agente
- Nome utente e password dell'account utente creato per l'agente
- Chiave di autenticazione agente impostata

Per installare un agente per un host Windows

1. Fare doppio clic sull'utilità di avvio di installazione dell'agente.

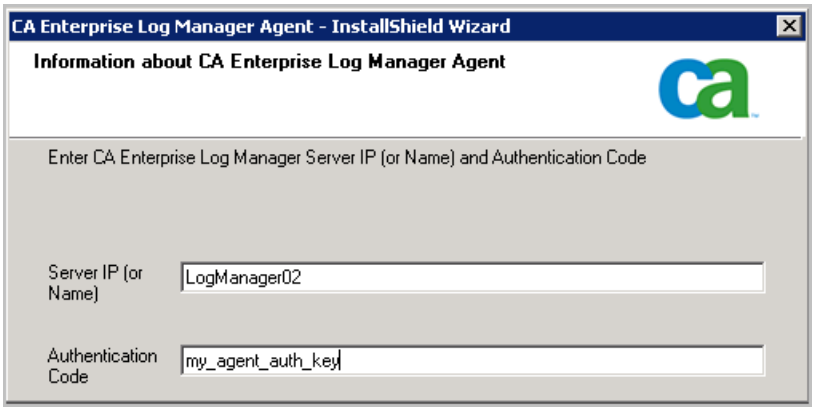
Viene avviata l'installazione guidata.

2. Fare clic su Avanti, leggere la licenza, selezionare accettare i termini del contratto di licenza per continuare e fare nuovamente clic su Avanti.
3. Accettare il percorso di installazione o modificarlo e fare clic su Avanti.
4. Immettere le informazioni richieste nel modo seguente:
   a. Inserire il nome host del CA Enterprise Log Manager a cui questo agente deve inoltrare i registri che raccoglie.

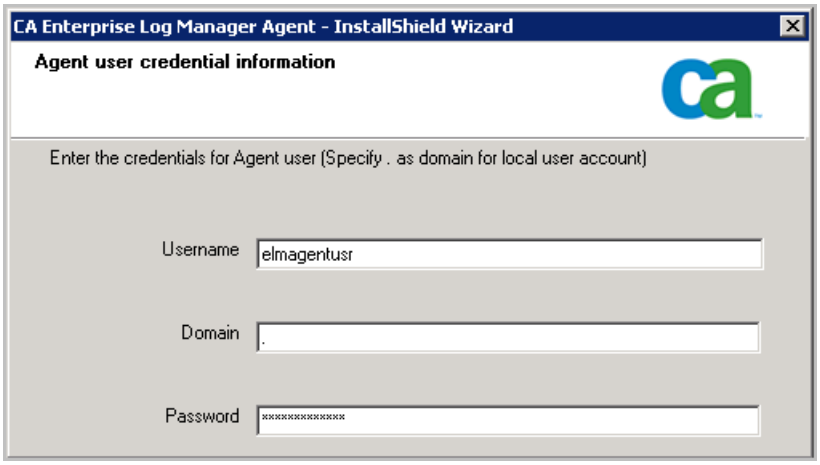
      Nota: dato che in questo scenario di esempio il CA Enterprise Log Manager utilizza DHCP per l'assegnazione dell'indirizzo IP, quest'ultimo non dovrebbe essere inserito. Inserendolo, si correrebbe il rischio di dover reinstallare l'agente se l'indirizzo IP del server dovesse cambiare.

   b. Immettere la chiave di autenticazione agente.

   Di seguito un esempio:



5. Immettere il nome e la password definiti nell'account utente impostato per l'agente e fare clic su Avanti.



6. Fare clic su Avanti. Non è obbligatorio specificare un file connettore esportato.

   Viene visualizzata la finestra Avvia copia dei file.

7. Fare clic su Avanti.

   Il processo di installazione dell'agente è ora completo.

8. Fare clic su Fine.

9. Proseguire con la configurazione dei connettori per questo agente.

   Dopo aver configurato i connettori, gli eventi raccolti vengono inviati all'archivio registro eventi di CA Enterprise Log Manager tramite la porta 17001.

   Importante: Se non si consente il traffico in uscita dall'host su cui è stato installato l'agente e si utilizza Windows Firewall, è necessario aprire questa porta sul proprio Windows Firewall.

Ulteriori informazioni:

Download del programma di installazione dell'agente (a pagina 38)
Creare un account utente per l'agente (a pagina 36)
Impostare la chiave di autenticazione agente. (a pagina 37)

Creare un connettore basato su NTEventLog

Dopo aver installato un agente, creare un connettore per specificare le origini evento degli eventi da raccogliere. Dal momento che si è installato un agente su un server con un sistema operativo Windows, si crea un connettore basato sull'integrazione di NTEventLog e si specificano le impostazioni per WMILogSensor come descritto nella guida del connettore, che si apre dal programma di creazione guidata del nuovo connettore. Specificare il nome dell'host su cui l'agente è installato per la raccolta dei registri basata sull'agente. Se lo si desidera, è possibile aggiungere un altro sensore di registro WMI per il connettore e specificare un host diverso da quello su cui l'agente è installato. Questo consente la connessione ai registri priva di agenti. L'host o gli host aggiuntivi devono essere nello stesso dominio e avere lo stesso amministratore Windows del primo host aggiunto.

Per configurare un connettore basato su NTEventLog

1. Ingrandire il browser che visualizza l'Explorer agente di CA Enterprise Log Manager.
2. Espandere Explorer agente e poi Gruppo agenti predefinito.

   Verrà visualizzato il nome del computer su cui è stato installato l'agente.

3. Selezionare questo agente.

   Il pannello Connettori agente verrà visualizzato.

4. Fare clic su Crea nuovo connettore.

   La creazione guidata del nuovo connettore viene visualizzata con selezionato il passaggio relativo ai dettagli connettore.

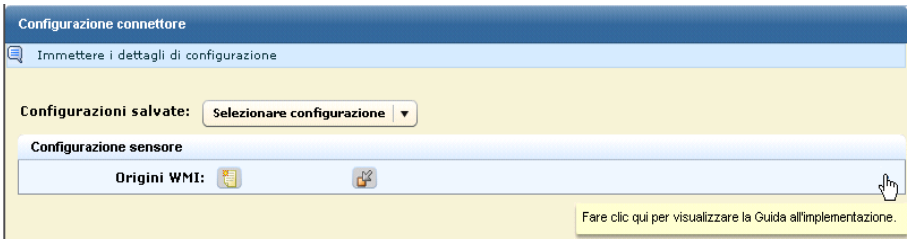
5. Lasciare selezionata l'opzione Integrazioni e selezionare NTEventLog dall'elenco a discesa Integrazione.

   I campi Nome connettore e Descrizione vengono popolati in base alla selezione dell'integrazione.

6. Modificare il nome del connettore per renderlo univoco. Considerare la possibilità di estendere questo nome con quello del server di destinazione, ad esempio NTEventLog_Connector_USER001LAB.

7. Selezionare il passaggio Configurazione connettore.

Verrà visualizzato il pannello Configurazione sensore, con un pulsante della guida in linea del connettore per NTEventLog, che fornisce aiuto per la compilazione dei campi per la configurazione del sensore.



8. Fare clic sul pulsante per la visualizzazione dei dettagli delle origini WMI.

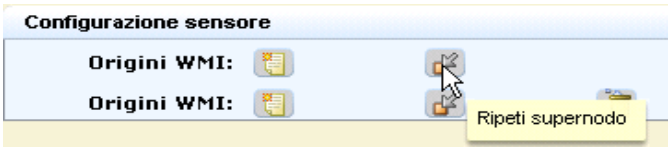
9. Configurare le impostazioni WMILogSensor per il computer locale per la raccolta di registri basata sugli agenti. Per ulteriori informazioni, fare clic sul link Aiuto.

   L'esempio seguente mostra una configurazione in cui l'utente è un amministratore Windows sul server WMI specificato. Il dominio è per il server WMI.

10. (Facoltativo) Utilizzare lo stesso connettore per configurare un sensore WMI per un computer diverso per la raccolta registri priva di agenti.

    a. Fare clic sul pulsante Ripeti supernodo.

    Nella figura seguente viene mostrata una configurazione con due origini WMI.



    b. Configurare le impostazioni WMILogSensor per un altro computer.

    Nell'esempio seguente viene mostrata la configurazione per un secondo sensore di registro WMI nello stesso dominio e con le stesse credenziali di amministratore.

11. Fare clic su Salva e chiudi.

12. Per visualizzare lo stato del connettore configurato, eseguire le seguenti operazioni:

    a. Selezionare l'agente nel riquadro di sinistra.

    b. Fare clic su Stato e comando.

    c. Selezionare Visualizza stato dei connettori.

    Verrà visualizzato il pannello Dettagli di stato.

13. Fare clic sul link In esecuzione.

    Lo stato visualizzato dalla destinazione configurata nel connettore include la percentuale CPU, l'utilizzo della memoria e la media di eventi al secondo (EPS, Events Per Second).

Configurare un'origine evento Windows

Dopo aver configurato un connettore utilizzando l'integrazione NTEventLog nell'agente, si dovrebbe essere in grado di visualizzare gli eventi attraverso il proprio Visualizzatore eventi. Se gli eventi non vengono inoltrati al proprio visualizzatore eventi, si devono modificare le impostazioni di Windows relative ai Criteri locali nell'origine evento.

Configurare i criteri locali nell'origine evento per un connettore NTEventLog

1. Se Explorer raccolta registri non è ancora stato visualizzato, fare clic sulla scheda Amministrazione.
2. Espandere Libreria di perfezionamento eventi, Integrazioni, Sottoscrizione, selezionare NTEventLog e fare clic sul link Aiuto sopra a Nome integrazione nel pannello Visualizza dettagli integrazione.

   Viene visualizzata la Guida al connettore per NT Event Log (Sicurezza, Applicazione, Sistema).
3. Ridurre l'interfaccia utente CA Enterprise Log Manager e seguire le indicazioni nella Guida al connettore per modificare i criteri locali su un'origine evento che viene eseguita in un sistema operativo Windows.

   Nota: per il sistema Windows Server 2003, selezionare Pannello di controllo, Strumenti di amministrazione, Criteri di protezione locali, quindi espandere i criteri locali.
4. (Facoltativo) Se si configura un sensore WMI per un secondo server WMI, modificare i criteri locali anche su quel server.
5. Ridurre CA Enterprise Log Manager.

Visualizzazione dei registri dalle origini evento di Windows

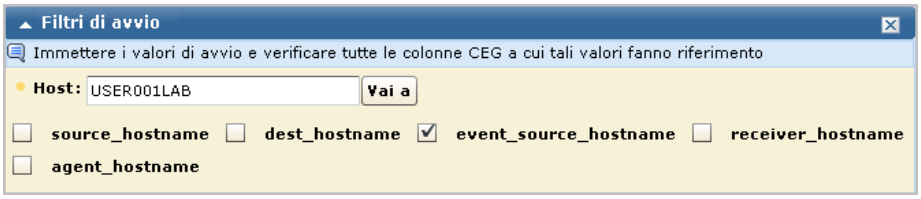
Uno dei modi più veloci per visualizzare i risultati delle query negli eventi in ingresso è utilizzare il Prompt dell'host. È anche possibile selezionare query o rapporti.

Per visualizzare i registri eventi in arrivo

1. Selezionare la scheda Query e rapporti.

   Viene visualizzata la sottoscheda Query.
2. Espandere i prompt sotto Elenco Query e selezionare Host.

3. Immettere il nome del server WMI configurato per il sensore nel campo Host. Togliere gli altri segni di spunta e fare clic su Vai a.



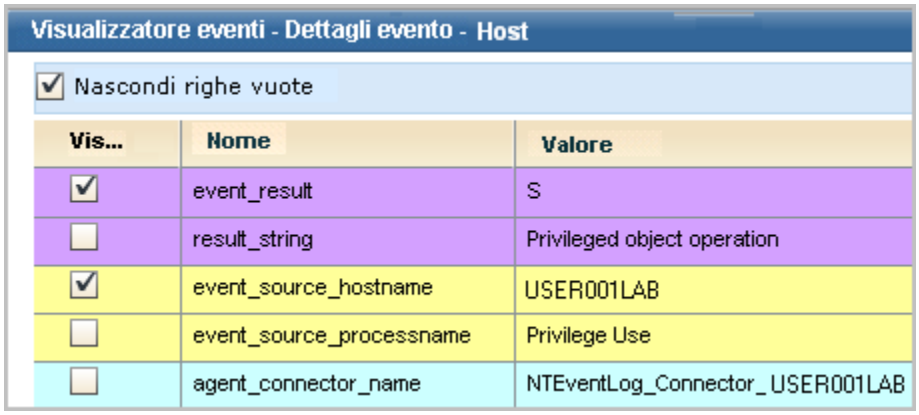
Vengono visualizzati gli eventi provenienti dalle origini evento del server WMI.

4. Fare clic su CA Severity e scorrere l'elenco alla ricerca di un avviso. Ecco un piccolo esempio, senza le colonne Data e Origine evento:

Livello di gravità CA	Utente di origine	Risultato	Categoria	Azione	Nome log
Avviso	calm_agent	S	System Access	Privilege Use	NT-Security

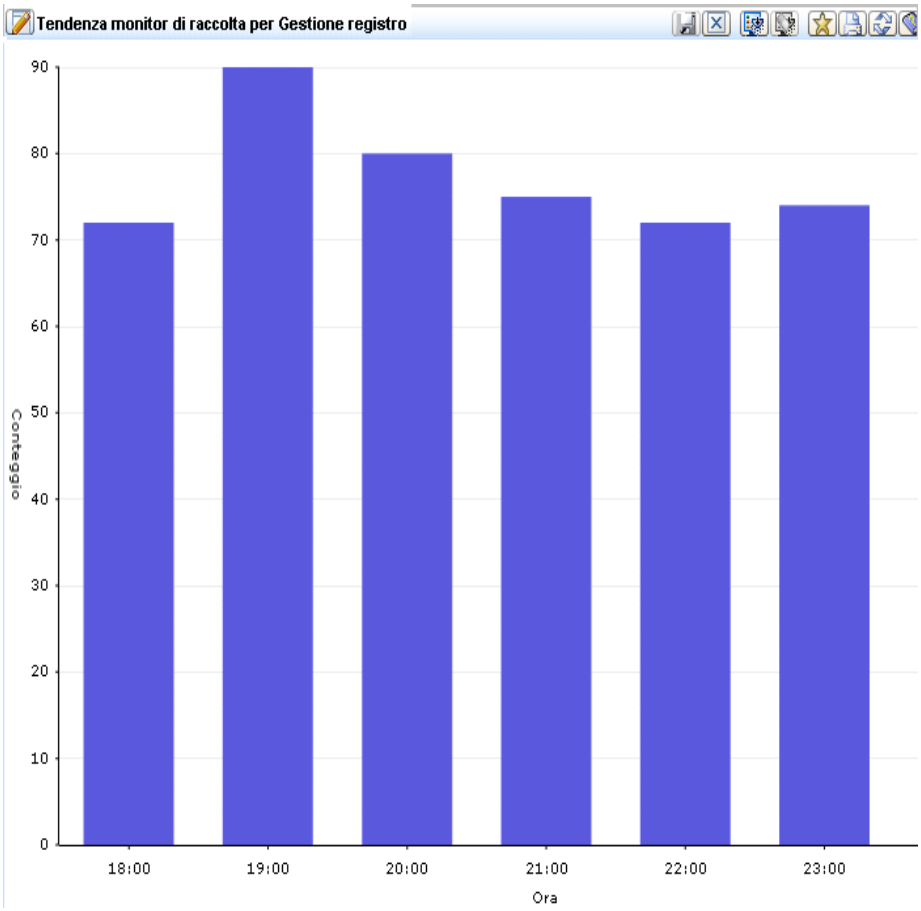
5. Fare clic su Mostra eventi non elaborati per visualizzare gli eventi non elaborati dell'avviso.

6. Fare doppio clic sull'avviso per visualizzare il Visualizzatore eventi con molti più dati. Ecco qualche riga di dati di esempio:



Vis...	Nome	Valore
☑	event_result	S
☐	result_string	Privileged object operation
☑	event_source_hostname	USER001LAB
☐	event_source_processname	Privilege Use
☐	agent_connector_name	NTEventLog_Connector_USER001LAB

7. Fare clic sulla scheda Query e rapporti e selezionare una query da Elenco query, ad esempio Tendenza monitor di raccolta per Gestione registro. Visualizzare il grafico a colonne risultante.



8. Fare clic su Rapporti. In Elenco rapporti, inserire "auto" nel campo Cerca per visualizzare il nome report Eventi di automonitoraggio di sistema. Selezionare questo rapporto per visualizzare un elenco degli eventi generati dal server CA Enterprise Log Manager.

Nota: per informazioni sulla pianificazione dei rapporti relativi alle informazioni che si desidera analizzare, consultare la *Guida all'amministrazione*.

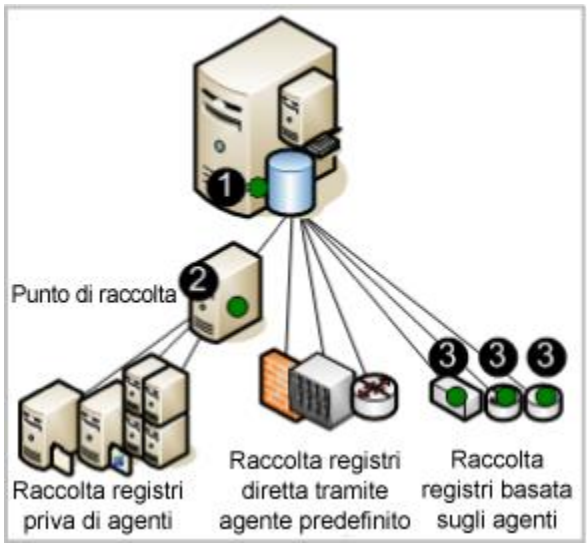
Capitolo 4: Funzionalità principali

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

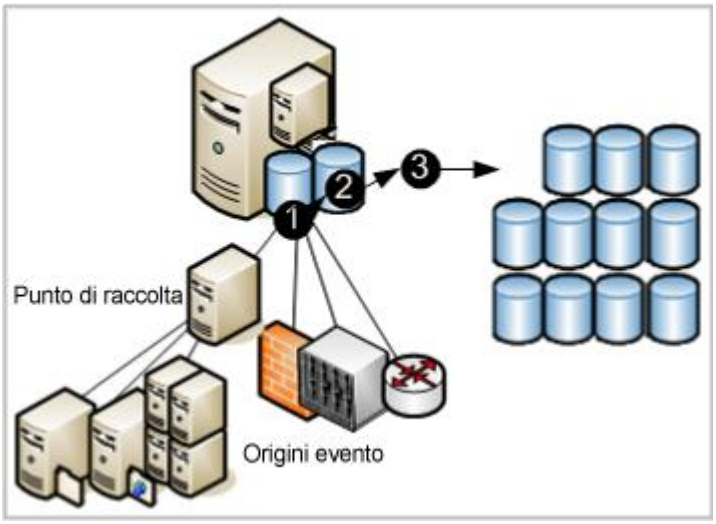
  Con la raccolta basata su agenti, viene installato un agente dove una o più origini di eventi sono in esecuzione ed è configurato un connettore per ogni origine di evento.

  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

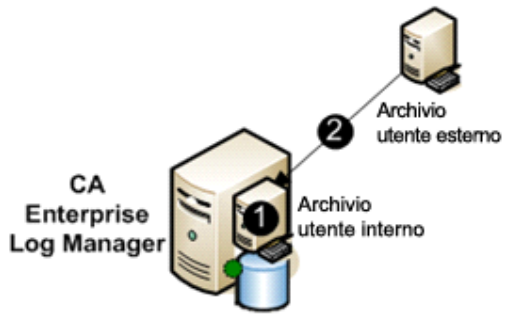
Gli elenchi con chiave possono essere aggiornati manualmente, importando un file o eseguendo una procedura CA IT PAM di valori dinamici.

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

Gestione delle adesioni

Al momento di configurare l'archivio utenti, si sceglie se utilizzare l'archivio utenti predefinito su CA Enterprise Log Manager per impostare gli account utente o fare riferimento a un archivio utenti esterno dove gli account utente sono già definiti. Il database sottostante è un'esclusiva di CA Enterprise Log Manager e non utilizza un DBMS commerciale.

Gli archivi utente esterni supportati includono CA SiteMinder e le directory LDAP, come Microsoft Active Directory, Sun One e Novell eDirectory. Se si fa riferimento a un archivio utenti esterno, le informazioni sull'account dell'utente vengono caricate automaticamente in formato di sola lettura, come illustrato dalla freccia nel diagramma seguente. Solo i dettagli specifici dell'applicazione vengono definiti per gli account selezionati. Nessun dato viene spostato dall'archivio utenti interno all'archivio utenti esterno di riferimento.



I numeri nella figura si riferiscono a questi passaggi:

1. L'archivio utenti interno esegue la gestione delle adesioni tramite l'autenticazione delle credenziali fornite dagli utenti al momento dell'accesso; autorizza inoltre gli utenti ad accedere a diverse funzioni dell'interfaccia utente sulla base dei criteri associati ai ruoli assegnati ai loro account utente. Se il nome utente e la password dell'utente che cerca di eseguire l'accesso sono stati caricati da un archivio utenti esterno, le credenziali inserite devono corrispondere a quelle caricate.
2. L'archivio utenti esterno ha come unica funzione il caricamento degli account utente sull'archivio utenti interno. Il caricamento viene eseguito automaticamente quando viene salvato il riferimento all'archivio utenti.

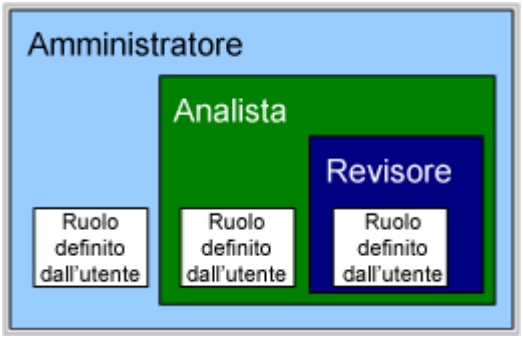
Nota: per informazioni sulla configurazione dell'accesso utente di base, consultare la *Guida all'implementazione CA Enterprise Log Manager*. Per informazioni sui criteri che supportano ruoli predefiniti, sulla creazione di account utente e sull'assegnazione di ruoli, consultare la *Guida all'amministrazione 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.

Contenuti in dotazione

CA Enterprise Log Manager include contenuti predefiniti che è possibile utilizzare non appena si installa e configura il prodotto. La procedura di sottoscrizione aggiunge regolarmente nuovi contenuti, aggiornando i contenuti esistenti.

Le categorie di contenuti predefiniti includono:

- Rapporti con tag
- Query con tag
- Integrazioni con sensori associati, file di analisi (XMP), file di mapping (DM) e, in alcuni casi, regole di soppressione
- Regole di soppressione e riepilogo

Capitolo 5: Ulteriori informazioni su CA Enterprise Log Manager

Questa sezione contiene i seguenti argomenti:

Visualizzazione dei tooltip

È possibile identificare le funzioni di pulsanti, caselle di controllo e rapporti sulla pagina di CA Enterprise Log Manager nella visualizzazione corrente.

Per visualizzare tooltip e altri aiuti

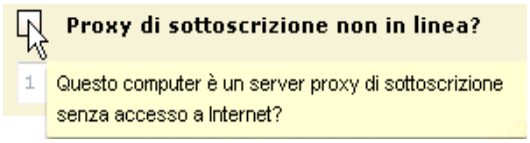
1. Spostare il cursore sui pulsanti per visualizzare la descrizione della relativa funzione. In questo modo è possibile visualizzare la funzione di tutti i pulsanti.

2. Notare la differenza tra i pulsanti attivi e quelli inattivi.

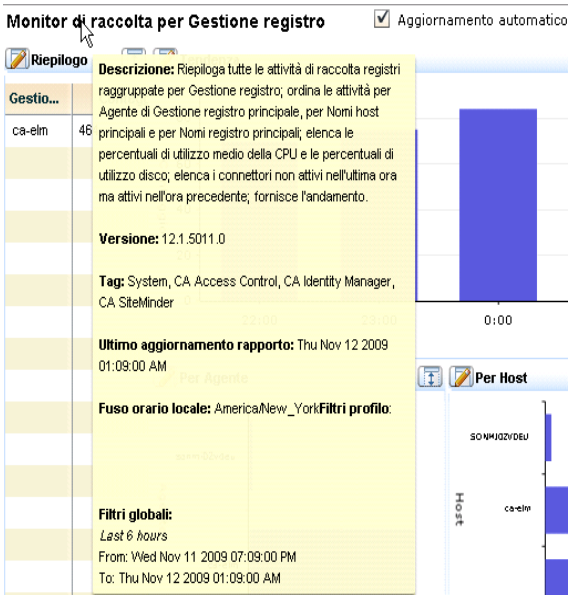
   I pulsanti attivi abilitati sono visualizzati a colori. Ad esempio, gli amministratori della gestione di utenti e accessi visualizzano il pulsante Elenco filtri di accesso a colori.

   I pulsanti inattivi disabilitati sono visualizzati in bianco e nero. Ad esempio, gli auditor visualizzano il pulsante Elenco filtri di accesso in bianco e nero.

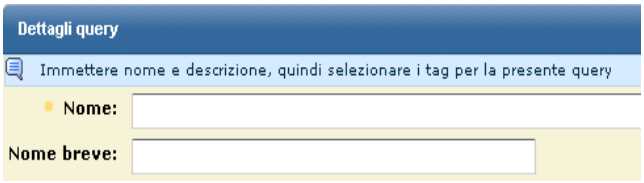
3. Visualizzare le descrizioni relative ai campi di inserimento o alle caselle di controllo spostando il cursore sul nome del campo.



4. Visualizzare le descrizioni dei rapporti spostando il cursore sul nome del rapporto.



5. Notare il puntino arancione che si trova a sinistra di alcuni campi. Indica che il campo è obbligatorio. In caso di configurazioni che è possibile salvare, il salvataggio non è consentito fino a quando tutti i campi obbligatori non sono stati compilati.



Visualizzare la Guida in linea

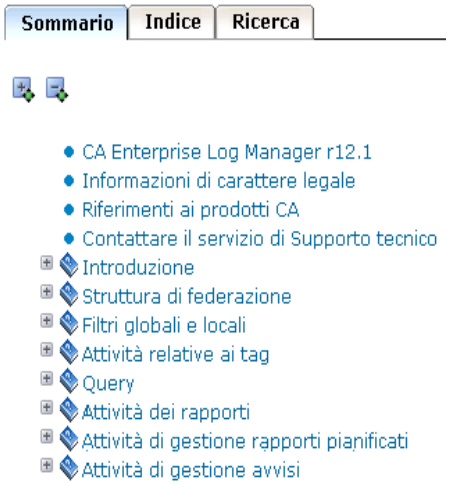
È possibile visualizzare la Guida in linea per la pagina visualizzata o per qualsiasi attività si desideri svolgere.

Per visualizzare la Guida in linea

1. Fare clic sul link Aiuto nella barra degli strumenti per visualizzare l'applicazione Guida in linea di CA Enterprise Log Manager.

   Si aprirà la Guida in linea di CA Enterprise Log Manager, i cui contenuti vengono visualizzati nel riquadro a sinistra.

2. Accedere alla guida sensibile al contesto dal pulsante Aiuto come mostrato nell'esempio seguente.

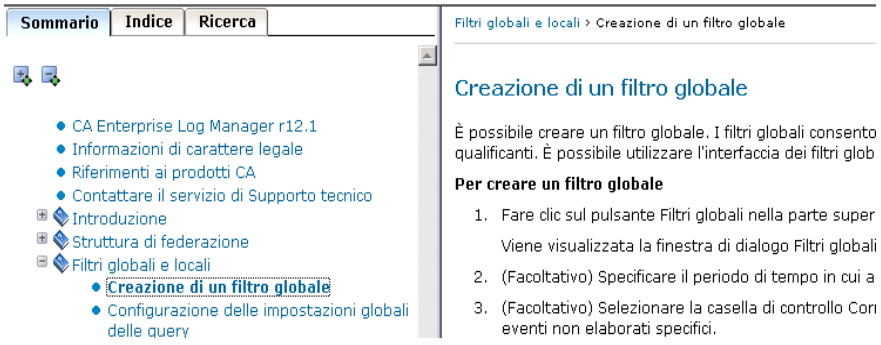
   a. Fare clic sul pulsante Visualizza / Modifica filtri globali.

   Verrà visualizzata la finestra Filtri e impostazioni globali, assieme a un pulsante Aiuto.

   b. Fare clic sul pulsante Aiuto. La Guida in linea per la procedura da eseguire nella pagina, riquadro o finestra di dialogo corrente viene visualizzata in una finestra secondaria.

   c. Se si conosce l'attività da eseguire, ma non si sa come accedere alla pagina corrispondente in CA Enterprise Log Manager, tale pagina potrebbe essere elencata nel Sommario. Facendo clic sul titolo dell'attività è possibile visualizzare la pagina.

   Nota: se non è possibile trovare l'attività richiesta nel Sommario, fare riferimento al bookshelf di documentazione.

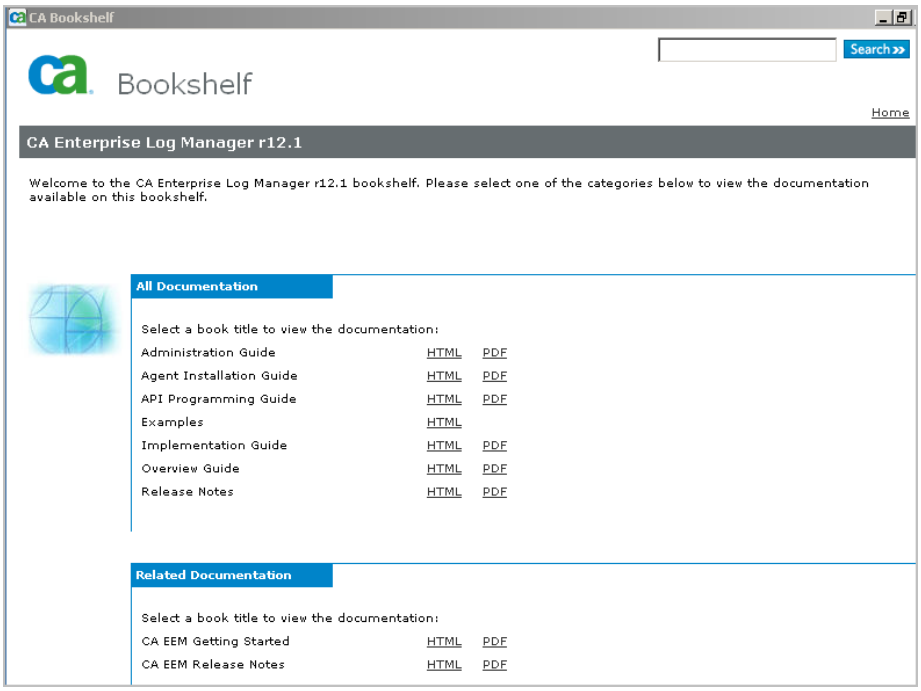
Esplorazione della Bookshelf della documentazione

È possibile copiare la bookshelf nel disco rigido locale e aprire qualsiasi libro in formato HTML o PDF. I libri in formato HTML contengono riferimenti incrociati tra libri.

Per esplorare la bookshelf

1. Copiare la Bookshelf nell'unità locale dal DVD di installazione dell'applicazione o scaricarla dal sito Web dell'assistenza clienti di CA. Fare doppio clic su Bookshelf.hta o su Bookshelf.html per aprire la bookshelf.

   Verrà visualizzata una pagina simile alla seguente:

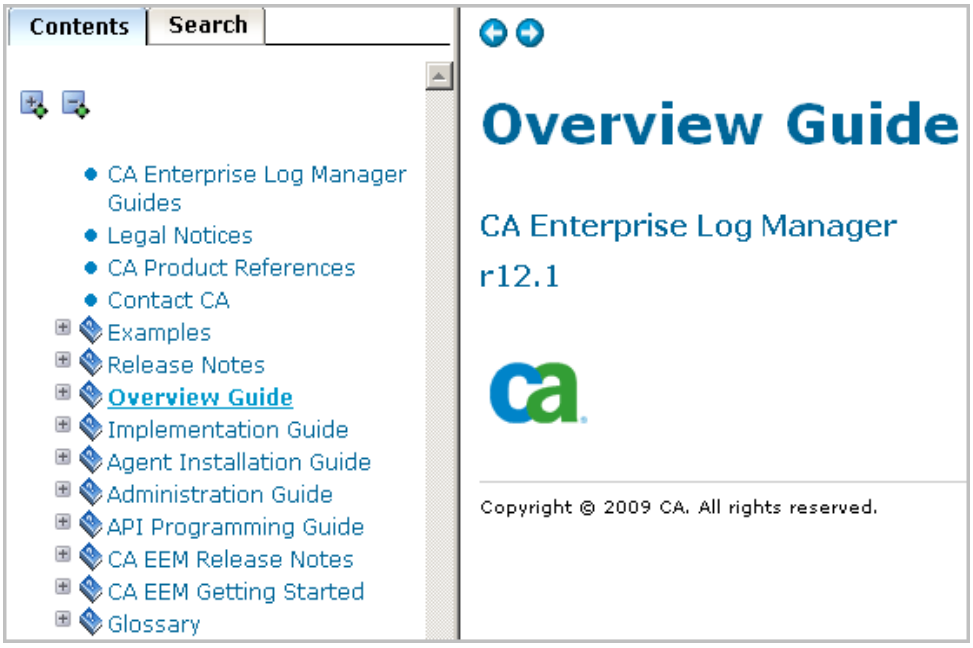


   Seguono le descrizioni del contenuto delle guide principali accompagnate da esempi:

Documentazione	Descrive come
Guida all'installazione degli agenti	Installare agenti
Guida all'implementazione	Installare e configurare un sistema CA Enterprise Log Manager.

Documentazione	Descrive come
Guida all'amministrazione	Personalizzare la configurazione, eseguire attività amministrative di routine e utilizzare query, rapporti e avvisi.
Guida alla programmazione API	Utilizzare l'API per visualizzare i dati di evento in un browser Web o per integrare i rapporti in un altro prodotto CA o di terze parti.
Esempi	Risolvere problemi aziendali comuni, con i collegamenti agli argomenti della documentazione.

2. Immettere un valore nel campo Ricerca e fare clic sul pulsante Cerca per visualizzare tutte le corrispondenze con i criteri inseriti.
3. Fare clic su un link Stampa per aprire il PDF della guida selezionata.
4. Fare clic su un link HTML per aprire il set di documentazione integrato. Il set integrato include tutte le guide nel formato HTML. Se si seleziona il link HTML della Guida generale, viene visualizzata la guida stessa.



Glossario

accesso dati

Accesso dati è un tipo di autorizzazione conferita a tutti i CA Enterprise Log Manager sfruttando il Criterio predefinito di accesso ai dati., nella classe di risorsa di CALM. Ogni utente può accedere a tutti i dati, a meno che non lo si impedisca mediante dei filtri di accesso.

Accesso ODBC e JDBC

L'*accesso ODBC e JDBC* agli archivi di registro eventi di CA Enterprise Log Manager supporta l'utilizzo dei dati di evento con svariati prodotti di terze parti, inclusa la creazione di rapporti eventi personalizzati con strumenti di terze parti, la correlazione di eventi mediante motori di correlazione e la valutazione degli eventi tramite prodotti per il rilevamento di violazioni o malware. I sistemi Windows utilizzano l'accesso ODBC; i sistemi UNIX e LINUX utilizzano l'accesso JDBC.

account

Un *account* è un utente globale che è anche un utente dell'applicazione CALM. Un singolo individuo può disporre di più di un account, ognuno dei quali dotato di un diverso ruolo definito dall'utente.

adapter CA

Gli *adapter CA* sono un gruppo di listener che riceve eventi da componenti di CA Audit come i client di CA Audit e i recorder iRecorder e SAPI, oltre ad essere le origini che inviano nativamente gli eventi con iTechnology.

agente

Un *agente* è un servizio generico configurato con dei connettori, ognuno dei quali raccoglie eventi non elaborati da una singola origine evento per poi inviarli a CA Enterprise Log Manager per l'elaborazione. Ogni CALM> è dotato di un agente integrato. Inoltre, è possibile installare un agente su un punto di raccolta remoto e raccogliere gli eventi negli host in cui non si possono installare agenti. È possibile anche installare un agente su un host in cui si eseguono le origini evento, e poter quindi applicare le regole di soppressione e crittografare la trasmissione a CA Enterprise Log Manager.

agente predefinito

L'*agente predefinito* è l'agente che viene installato con il server CA Enterprise Log Manager. Può essere configurato per la raccolta diretta di eventi syslog nonché per la raccolta da diverse origini eventi non syslog come CA Access Control r12 SP1, Servizi di certificazione Microsoft Active Directory e database Oracle9i.

aggiornamenti di contenuto

Gli aggiornamenti di contenuto sono le parti non binarie degli aggiornamenti di sottoscrizione salvati nel server di gestione CA Enterprise Log Manager. Gli aggiornamenti di contenuto comprendono contenuti come i file XMP e DM, gli aggiornamenti di configurazione per i moduli di CA Enterprise Log Manager e gli aggiornamenti della chiave pubblica.

aggiornamenti di sottoscrizione

Gli aggiornamenti di sottoscrizione sono i file binari e non, distribuiti dal server di sottoscrizione diCA. I file binari sono degli aggiornamenti di modulo di prodotto solitamente installati sui CA Enterprise Log Manager. I file non binari, o aggiornamenti di contenuto, vengono memorizzati sul server di gestione.

aggregazione evento

L'aggregazione evento è il processo di consolidamento delle voci di registro simili fra loro in una singola voce contenente il numero di ricorrenze dell'evento. Le regole di riepilogo definiscono la modalità di aggregazione degli eventi.

analisi

L'analisi, detta anche analisi del messaggio, è il processo di acquisizione dei dati non elaborati di dispositivo allo scopo di trasformarli in coppie chiave-valore. L'analisi si esegue usando un file XMP. L'analisi, che precede il mapping dei dati, è un passo del procedimento di integrazione, che trasforma gli eventi non elaborati raccolti da un'origine evento in un evento perfezionato che si può visualizzare.

analisi dei file XMP

L'analisi dei file XMP è il procedimento eseguita dall'utility di Analisi del messaggio per individuare tutti gli eventi contenenti ogni stringa di corrispondenza preliminare. Si dividerà quindi ogni evento corrispondente in token in modo da poterlo analizzare utilizzando il primo filtro individuato che utilizzi la medesima stringa di corrispondenza preliminare.

analisi del mapping

L'*analisi del mapping* è un passaggio nella procedura guidata File di mapping che consente di verificare ed eseguire delle modifiche ad un file di mapping dei dati. Gli eventi campione vergono verificati tramite il file di mapping dei dati, ed i risultati si convalidano con la CEG.

analisi di messaggio

L'analisi di messaggio è il processo di applicazione delle regole all'analisi di un registro di eventi non elaborati, in modo da ottenere informazioni specifiche come il timestamp, l'indirizzo IP ed il nome utente. Le regole di analisi utilizzano la corrispondenza dei caratteri per individuare un preciso testo di evento e collegarlo ai valori selezionati.

analisi di registro

L'analisi di registro è il procedimento di estrazione dei dati da un registro, in modo che i valori analizzati possano essere utilizzati in una fase successiva della gestione di registro.

analisi di registro

L'analisi di registro è lo studio delle voci di registro utile per identificare gli eventi d'interesse. Se i registri non vengono analizzati in maniera tempestiva, il loro valore si riduce significativamente.

applicazione software

L'*applicazione software* contiene un componente del sistema operativo ed il componente software di CA Enterprise Log Manager.

AppObject

Gli *AppObject,* o oggetti applicazione, sono risorse specifiche di prodotto memorizzate in CA EEM sotto l'istanza applicazione di un dato prodotto. Per l'istanza applicazione di CAELM, tali risorse comprendono i contenuti di rapporto e di query, le attività pianificate per i rapporti e gli avvisi, i contenuti e le configurazioni degli agenti, le configurazioni di servizi, adapter ed integrazioni, i file di mapping dei dati e di analisi del messaggio e le regole di soppressione e di riepilogo.

archiviazione automatica

L'archiviazione automatica è un procedimento configurabile che consente di automatizzare lo spostamento dei database di archivio da un server all'altro. Nella prima fase dell'archiviazione automatica, il server di raccolta invia al server di rapporto i database appena archiviati, ad intervalli specificati dall'utente. Nella seconda fase, il server di rapporto invia i database invecchiati al server di archiviazione remota per archiviarli a lungo termine, eliminando così la necessità di eseguire un backup manuale e la procedura di spostamento. Per eseguire un'archiviazione automatica, l'utente dovrà configurare un'autenticazione priva di password dal server di origine a quello di destinazione.

archiviazione di registro

L'archiviazione di registro è il processo che si verifica quando il database hot raggiunge le sue dimensioni massime, pur avendo eseguito la compressione di riga e dopo aver cambiato stato da hot a warm. Gli amministratori devono eseguire manualmente un backup dei database warm prima che sia raggiunta la soglia di eliminazione, oltre a dover eseguire l'utility LMArchive per registrare il nome dei backup. Archivia query consentirà quindi di visionare questa informazione.

archivio di catalogo

Consultare il catalogo.

archivio registro eventi

L'*archivio registro eventi* è un componente del server CA Enterprise Log Manager in cui gli eventi in arrivo si archiviano nei database. Occorre creare manualmente un backup dei database dell'archivio registro eventi, per poi spostarli su una soluzione remota di archiviazione dei registri prima dell'ora stabilita per l'eliminazione. È possibile ripristinare i database archiviati in un archivio registro eventi.

archivio registro eventi

L'archivio registro eventi è il risultato del processo di archiviazione, in cui l'utente esegue il backup di un database warm ed invia una notifica a CA Enterprise Log Manager con l'utility LMArchive. Fatto ciò, il database sottoposto a backup passerà dall'archivio registro eventi all'archivio a lungo termine.

archivio utente

Un *archivio utente* è il repository delle informazioni utente e dei criteri di password globali. Per impostazione predefinita, l'archivio utente di CA Enterprise Log Manager è il repository locale. È possibile anche configurarlo in modo da fare riferimento a CA SiteMinder o ad una directory LDAP supportata come Microsoft Active Directory, Sun One o Novell eDirectory. Indipendentemente dal modo in cui si configura l'archivio utente, il repository locale sul server di gestione contiene informazioni specifiche di applicazione sugli utenti, come ad esempio il ruolo utente e i criteri di accesso associati.

avviso

Un *avviso* è un processo pianificato di query che è possibile utilizzare per individuare le violazioni di criterio, le tendenze di utilizzo, gli schemi di accesso e le altre informazioni che richiedono attenzione a breve termine. Per impostazione predefinita, quando la query di avviso restituisce risultati, essi verranno visualizzati nella pagina degli avvisi di CA Enterprise Log Manager e quindi aggiunti ad un feed RSS. Quando si pianifica un avviso, è possibile specificare destinazioni aggiuntive, come ad esempio la posta elettronica, un processo CA IT PAM di output di evento/avviso e i trap SNMP.

CA Enterprise Log Manager

CA Enterprise Log Manager è una soluzione utile per raccogliere i registri da origini evento di tipi diversi ed ampiamente distribuite, per verificare la conformità con le query e con i rapporti e per tener traccia dei database di registri compressi trasferiti su soluzioni esterne di archiviazione a lungo termine.

CA IT PAM

CA IT PAM corrisponde alla forma abbreviata di CA IT Process Automation Manager. Questo prodotto CA automatizza i processi definiti dall'utente. CA Enterprise Log Manager utilizza due processi: la creazione di un processo di output evento/avviso per un prodotto locale, come CA Service Desk, ed il processo di creazione dinamica di elenchi che possono essere importati come valori chiave. Per eseguire l'integrazione, è necessario disporre di CA IT PAM r2.1.

CA Spectrum

CA Spectrum è un prodotto di gestione degli errori di rete che è possibile integrare con CA Enterprise Log Manager per l'utilizzo come destinazione di avvisi inviati sottoforma di trap SNMP.

CAELM

CAELM è il nome di istanza applicazione che CA EEM utilizza per CA Enterprise Log Manager. Per accedere alle funzionalità di CA Enterprise Log Manager di CA Embedded Entitlements Manager, inserire l'URL https://<ip_address>:5250/spin/eiam/eiam.csp, selezionare CAELM come nome di applicazione, ed inserire la password dell'utente EiamAdmin.

caelmadmin

Il nome utente e la password di *caelmadmin* sono credenziali necessarie per accedere al sistema operativo dell'applicazione software. L'ID utente caelmadmin viene creato durante l'installazione di questo sistema operativo. Durante l'installazione del componente software, l'installatore deve specificare la password di EiamAdmin, ovvero dell'account di super utente di CA EEM. La stessa password verrà assegnata anche all'account caelmadmin. Si consiglia all'amministratore del server di accedere via ssh come utente caelmadmin, e di modificare la password predefinita. Anche se l'amministratore non può accedere via ssh come utente principale, potrà passare gli utenti all'account principale con il relativo comando (su root).

caelmservice

caelmservice è un account di servizio utile per eseguire iGateway ed i servizi locali di CA EEM come utente non principale. L'account caelmservice si utilizza per installare gli aggiornamenti del sistema operativo scaricati insieme agli aggiornamenti di sottoscrizione.

calendario

Un *calendario* consente di limitare il tempo di effettiva applicazione di un criterio d'accesso. Un criterio consente alle identità specificate di eseguire azioni su una risorsa in un certo periodo di tempo.

CALM

CALM è una classe di risorsa predefinita che comprende le seguenti risorse di CA Enterprise Log Manager: avviso, ArchiveQuery, calmTag, dati, EventGrouping, integrazione e rapporto. Le azioni consentite su questa classe di risorsa sono Annotazione (rapporti), Creazione (avviso, calmTag, EventGrouping, integrazione e rapporto), Dataaccess (Dati), Esecuzione (ArchiveQuery) e Pianificazione (avviso, rapporto).

calmTag

calmTag è un attributo di AppObject dotato di nome, che si utilizza creando un criterio di scoping per limitare gli utenti all'utilizzo di rapporti e query appartenenti a determinati tag. Tutti i rapporti e le query sono AppObject, e possono avere calmTag come attributo (non si deve confondere con il tag risorsa).

Campi CEG

I campi CEG sono etichette utilizzate per standardizzare la presentazione dei campi di eventi non elaborati provenienti da diverse origini evento. Durante il perfezionamento degli eventi, CA Enterprise Log Manager analizza i messaggi degli eventi non elaborati ottenendo una serie di coppie nome/valore e mappa i nomi degli eventi non elaborati ai campi CEG standard. Questo perfezionamento crea delle coppie nome/valore che consistono in campi e valori CEG provenienti dall'evento non elaborato. In altre parole, quando si perfezionano gli eventi non elaborati, le diverse etichette utilizzate in essi per lo stesso oggetto dati o elemento di rete vengono convertiti allo stesso nome di campo CEG. I campi CEG verranno mappati agli OID nella MIB utilizzata per i trap SNMP.

cartella

Una *cartella* è la posizione di un percorso di directory utilizzati dal server di gestione CA Enterprise Log Manager per memorizzare i tipi oggetto di CA Enterprise Log Manager. Nei criteri di scoping è possibile far riferimento alle cartelle per consentire o negare agli utenti di accedere ad un tipo di oggetto specifico.

catalogo

Il *catalogo* è il database in cui ogni CA Enterprise Log Manager conserva lo stato dei database archiviati, agendo anche come un indice di alto livello su tutti i database. Le informazioni di stato (warm, cold o defrosted) verranno mantenute per tutti i database presenti in questo CA Enterprise Log Manager e per qualsiasi altro database ripristinato in questo CA Enterprise Log Manager come defrosted. Le funzionalità di indicizzazione si estendono a tutti i database hot e warm nell'archivio registro eventi di questo CA Enterprise Log Manager.

categorie di evento

Le categorie di evento sono i tag utilizzati da CA Enterprise Log Manager per classificare gli eventi in base alla loro funzione, prima di inserirli nell'archivio eventi.

certificati

I *certificati* predefiniti utilizzati da CA Enterprise Log Manager sono CAELMCert.cer e CAELM_AgentCert.cer. Tutti i servizi CA Enterprise Log Manager utilizzano CAELMCert.cer per la comunicazione con il server di gestione. Tutti gli agenti utilizzano CAELM_AgentCert.cer per la comunicazione con i server di raccolta.

client di sottoscrizione

Un *client di sottoscrizione* è un server CA Enterprise Log Manager in grado di ottenere aggiornamenti di contenuto da un altro server CA Enterprise Log Manager, denominato server proxy di sottoscrizione. I client di sottoscrizione sondano regolarmente i server proxy di sottoscrizione configurati, e prelevano i nuovi aggiornamenti quando sono disponibili. Dopo aver prelevato gli aggiornamenti, il client installa i componenti scaricati.

componenti di visualizzazione

I componenti di visualizzazione sono opzioni utili per visualizzare i dati di rapporto fra cui una tabella, un diagramma (a linee, a barre, a colonne e a torta), oppure un visualizzatore eventi.

configurazione globale

La *configurazione globale* è una serie di impostazioni che si applica a tutti i serverCA Enterprise Log Manager che utilizzano il medesimo server di gestione.

configurazione salvata

Una *configurazione salvata* è una configurazione archiviata con i valori degli attributi di accesso ai dati di un'integrazione, che si può utilizzare come modello per creare una nuova integrazione.

connettore

Un *connettore* è un'integrazione per una particolare origine evento configurata su un dato agente. Un agente può caricare in memoria più connettori, di tipi simili o diversi. Il connettore consente la raccolta degli eventi non elaborati da un'origine e la trasmissione basata su regole degli eventi convertiti verso un archivio registro eventi, in cui essi saranno inseriti in un database hot. Le integrazioni out-of-the-box offrono una raccolta ottimizzata di una vasta gamma di origini evento, compresi i sistemi operativi, i database, i server Web, i firewall e molti altri tipi di applicazioni di protezione. È possibile definire un connettore per una propria origine evento da zero, oppure utilizzare un'integrazione come modello.

Contenuto dei trap SNMP

Un *trap SNMP* consiste in una serie di coppie nome/valore, in cui ogni nome è un OID (identificatore oggetto) ed ogni valore viene restituito da un avviso pianificato. I risultati di query restituiti da un avviso sono costituiti dai campi CEG e relativi valori. Il trap SNMP viene popolato sostituendo un OID per ogni campo CEG utilizzato per il nome della coppia nome/valore. La mappatura di ogni campo CEG a un OID viene memorizzata nella MIB. Il trap SNMP comprende solo le coppie nome/valore per i campi selezionati al momento di configurare l'avviso.

criterio di accesso

Un *criterio di accesso* è una regola che conferisce o nega ad un'identità (utente o gruppo utente) i diritti di accesso ad una risorsa applicazione. CA Enterprise Log Manager stabilisce se i criteri siano applicabili ad un utente specifico facendo corrispondere identità, risorse e classi di risorse, e valutando i filtri.

Criterio di accesso all'applicazione CALM

Il *Criterio di accesso all'applicazione CALM* è un tipo di elenco di controllo di accesso di un criterio di scoping che definisce chi può accedere a CA Enterprise Log Manager. Per impostazione predefinita, l'amministratore [di gruppo], l'analista [di gruppo] ed il revisore [di gruppo] potranno eseguire l'accesso.

criterio di delega

Un *criterio di delega* è un criterio di accesso che consente ad un utente di delegare la propria autorità ad un altro utente o ad un gruppo applicazione, globale o dinamico. È necessario eliminare esplicitamente i criteri di delega creati dall'utente eliminato o disattivato.

criterio di obbligo

Un *criterio di obbligo* è un criterio creato automaticamente insieme ad un filtro di accesso. Non si dovrebbe provare a creare, a modificare o ad eliminare direttamente un criterio di obbligo. Si consiglia invece di creare, di modificare o di eliminare il filtro d'accesso.

criterio di scoping

Un *criterio di scoping* è un tipo di criterio di accesso che conferisce o nega l'accesso alle risorse memorizzate nel server di gestione, come ad esempio AppObjects, utenti, gruppi, cartelle e criteri. Un criterio di scoping stabilisce quali identità possano accedere alle risorse specificate.

database archiviati

I *database archiviati* su un dato server CA Enterprise Log Manager comprendono tutti i database warm disponibili per le query per cui è necessario eseguire un backup manuale prima della scadenza, tutti i database cold registrati come sottoposti a backup e tutti quelli registrati come ripristinati dal backup.

defrosting

Il defrosting è il procedimento di modifica dello stato di un database da cold a defrosted. Questo processo viene eseguito da CA Enterprise Log Manager quando viene ricevuta una notifica dll'utility LMArchive relativa all'avvenuto ripristino di un database cold noto (se non si ripristina il database cold nel suo CA Enterprise Log Manager originale, non si dovrà utilizzare LMArchive ed eseguire il defrosting; con la ricatalogazione si aggiungerà il database ripristinato come database warm).

Destinazioni di trap SNMP

Quando si pianifica un avviso è possibile aggiungere una o più *destinazioni di trap SNMP*. Ogni destinazione di trap SNMP viene configurata con un indirizzo IP ed una porta. La destinazione è di solito un NOC o un server di gestione, come CA Spectrum o CA NSM. Quando le query per un processo di avviso pianificato restituiscono risultati verrà inviato un trap SNMP alle destinazioni configurate.

elementi di integrazione

Gli elementi di integrazione comprendono un sensore, un assistente di configurazione, un file di accesso dati ed uno o più file di analisi del messaggio (XMP) e di mapping dei dati.

elenco controllo di accesso identità

Un *elenco controllo di accesso identità* consente di specificare le diverse azioni che ogni identità selezionata può eseguire sulle risorse selezionate. Ad esempio, con un elenco di controllo accesso identità si può fare in modo che un'identità possa creare rapporti ed un'altra possa pianificarli ed annotarli. Un elenco controllo di accesso identità differisce da un elenco di controllo di accesso nel fatto che esso è incentrato sull'identità piuttosto che sulla risorsa.

event_action

event_action è il campo specifico di evento di quarto livello nella normalizzazione degli eventi utilizzata dalla CEG. Esso descrive azioni comuni. Avvio processo, Arresto processo ed Errore applicazione sono alcuni esempi di tipi di azioni evento.

event_category

event_category è il campo specifico di evento di secondo livello nella normalizzazione degli eventi utilizzata dalla CEG. Esso consente un'ulteriore classificazione degli eventi con uno specifico ideal_model. Alcuni tipi di categoria evento: Sicurezza operativa, Gestione identità, Gestione configurazione, Accesso alla risorsa e Accesso al sistema.

event_class

event_class è il campo specifico di evento di terzo livello nella normalizzazione degli eventi utilizzata dalla CEG. Esso consente un'ulteriore classificazione degli eventi in una specifica event_category.

eventi

Gli eventi in CA Enterprise Log Manager sono i record di registro generati da ogni origine evento specificata.

evento di automonitoraggio

Un *evento di automonitoraggio* è un evento registrato da CA Enterprise Log Manager. Le azioni eseguite dagli utenti entrati nel sistema, e le funzioni eseguite da diversi moduli, come i servizi e i listener, genereranno automaticamente questo tipo di eventi. È possibile visualizzare il rapporto di Dettagli eventi di automonitoraggio operazioni SIM selezionando un server di rapporto ed aprendo la scheda Eventi di automonitoraggio.

evento di osservazione

Un *evento di osservazione* è un evento che coinvolge un'origine, una destinazione ed un agente, in cui un agente di raccolta evento osserva e registra l'evento.

evento locale

Un *evento locale* è un evento che coinvolge una singola entità, in cui il medesimo host costituisce l'origine e la destinazione dell'evento. Un evento locale è il primo dei quattro tipi di evento utilizzati nella Grammatica evento comune.

evento nativo

Un *evento nativo* è lo stato o l'azione che attiva un evento non elaborato. È possibile ricevere ed analizzare o mappare gli eventi nativi come appropriato, per poi trasmetterli sotto forma di eventi perfezionati o non elaborati. Una mancata autenticazione è un evento nativo.

evento non elaborato

Un *evento non elaborato* è un'informazione attivata da un evento nativo inviata da un agente di monitoraggio al Log Manager collector. L'evento non elaborato viene spesso formattato come stringa syslog o come coppia nome-valore. In CA Enterprise Log Manager è possibile rivedere un evento nella sua forma non elaborata.

evento perfezionato

Un *evento perfezionato* è un'informazione evento mappata o analizzata che deriva da eventi non elaborati o riepilogati. CA Enterprise Log Manager esegue il mapping e l'analisi in modo che sia possibile ricercare le informazioni archiviate.

evento registrato

Si definiscono *evento registrato* le informazioni di evento non elaborate o perfezionate già inserite in un database. Gli eventi non elaborati vengono sempre registrati, a meno che non li si elimini o li si riepiloghi come avviene per gli eventi perfezionati. Si tratta di informazioni memorizzate e ricercabili.

evento remoto

Un *evento remoto* è un evento che coinvolge due diversi computer host, ovvero l'origine e la destinazione. Un evento remoto è il secondo dei quattro tipi di evento utilizzati nella Grammatica evento comune.

evento RSS

Un *evento RSS* è un evento generato da CA Enterprise Log Manager per convogliare un avviso verso prodotti ed utenti di terze parti. L'evento è un riepilogo del risultato di ogni avviso, ed un collegamento al file di risultato. È possibile configurare la durata di un dato elemento del feed RSS.

explorer agente

Explorer agente è l'archivio delle impostazioni di configurazione degli agenti (gli agenti si possono installare su un punto di raccolta o sugli endpoint in cui esistono delle origini evento).

federazione a coppie

Una *federazione a coppie* di server CA Enterprise Log Manager è una topologia che definisce una relazione paritaria fra server. Nella sua forma più semplice, il server 2 è figlio del server 1, ed il server 1 è figlio del server 2. Fra queste coppie di server vige una relazione a doppio senso. Si può definire una federazione a coppie per fare in modo che molti server siano peer l'uno dell'altro. Una query federata restituisce risultati dal server selezionato e da tutti i suoi peer.

federazione gerarchica

Una *federazione gerarchica* di server CA Enterprise Log Manager è una topologia che definisce una relazione gerarchica fra server. Nella sua forma più semplice, il server 2 è figlio del server 1, ma il server 1 non è figlio del server 2. Cioè, la relazione è a senso unico. Una federazione gerarchica può sfruttare più livelli di relazioni padre-figlio, mentre un singolo server padre può avere diversi server figlio. Una query federata produrrà risultati dai server selezionati e dai relativi figli.

file di analisi del messaggio (XMP)

Un *file di analisi del messaggio (XMP)* è un file XML, associato ad un tipo specifico di origine evento, che applica le regole di analisi. Le regole di analisi suddividono i dati rilevanti in un evento non elaborato in coppie nome-valore, che si potranno inviare al file di mapping dei dati per eseguire ulteriori elaborazioni. Questo tipo di file si utilizza in tutte le integrazioni e nei connettori, che si basano su di esse. Nel caso degli adapter CA, i file XMP si possono applicare anche al server CA Enterprise Log Manager.

file di mapping dei dati (DM)

I file di mapping dei dati (DM) sono file XML che utilizzano la Grammatica evento comune (CEG) di CA per trasformare gli eventi da un formato di origine ad uno conforme alla CEG, che sia possibile memorizzare nell'Archivio registro eventi a scopo di analisi e di creazione di rapporti. Ogni nome di registro deve disporre di un file DM prima di poter memorizzare i dati evento. Gli utenti possono modificare la copia di un file DM ed applicarla ad un determinato connettore.

filtraggio degli eventi

Il filtraggio degli eventi è il processo di rimozione degli eventi basato sui filtri di CEG.

filtro

Un *filtro* consente di porre dei limiti ad una query di archivio registro eventi.

filtro di accesso

Un *filtro di accesso* è un filtro che l'amministratore può impostare per controllare quali dati evento possano essere visualizzati dagli utenti e dai gruppi non amministrativi. Ad esempio, un filtro di accesso può ridurre i dati che alcune identità specifiche possono visualizzare in un rapporto. I filtri di accesso vengono convertiti automaticamente in criteri di obbligo.

filtro globale

Un *filtro globale* è un gruppo di criteri che possono essere specificati in modo da limitare ciò che viene mostrato in tutti i rapporti. Ad esempio, un filtro globale degli ultimi 7 giorni riporterà gli eventi generati negli ultimi sette giorni.

filtro locale

Un *filtro locale* è un gruppo di criteri che, visualizzando un rapporto, è possibile definire per limitare i dati mostrati dal rapporto corrente.

gestione agente

Gestione agente è il processo software che controlla tutti gli agenti associati ai CA Enterprise Log Manager federati. Può autenticare gli agenti con cui comunica.

gestione dei registri di protezione informatica

La definizione del NIST di *Gestione dei registri di protezione informatica* è la seguente: processo per generare, trasmettere, memorizzare, analizzare ed eliminare i dati di registro di protezione del computer.

gestione delle adesioni

La *gestione delle adesioni* consente di controllare ciò che gli utenti possono fare dopo l'autenticazione e l'ingresso nell'interfaccia di CA Enterprise Log Manager. È possibile ottenere tutto ciò con i criteri di accesso ed i ruoli assegnati agli utenti. I ruoli, o gruppi utente dell'applicazione, e i criteri di accesso possono essere di tipo predefinito o definito dall'utente. È l'archivio utente interno di CA Enterprise Log Manager ad occuparsi della gestione delle adesioni.

gruppo applicazione

Un *gruppo applicazione* è un gruppo specifico di prodotto che può essere assegnato ad un utente globale. I gruppi applicazione predefiniti perCA Enterprise Log Manager, o ruoli, sono amministratore, analista e revisore. Questi gruppi applicazione sono disponibili solo per gli utenti di CA Enterprise Log Manager, e non si possono assegnare agli utenti di altri prodotti registrati nel medesimo server di CA EEM. I gruppi di applicazione definiti dall'utente vanno aggiunti nel criterio di Accesso all'applicazione CALM predefinito, in modo che i suoi utenti possano accedere a CA Enterprise Log Manager.

gruppo di agenti

Un *Gruppo di agenti* è un tag che può essere applicato dagli utenti agli agenti selezionati, e che consente di applicare una configurazione agente a più agenti contemporaneamente, per poi recuperare i rapporti in base ai gruppi. Un dato agente può appartenere ad un solo gruppo alla volta. I gruppi di agenti si basano su criteri definiti dall'utente, come la regione geografica o l'importanza.

gruppo globale

Un *gruppo globale* è un gruppo condiviso fra istanze applicazioni registrate nel medesimo server di gestione di CA Enterprise Log Manager. È possibile assegnare qualsiasi utente ad uno o più gruppi globali. È anche possibile definire dei criteri di accesso con i gruppi globali come Identità a cui si consente o si impedisce di eseguire determinate azioni sulle risorse selezionate.

gruppo utenti

Un *gruppo utenti* può essere un gruppo applicazione, globale o dinamico. I gruppi applicazione predefiniti di CA Enterprise Log Manager sono amministratore, analista e revisore. Gli utenti CA Enterprise Log Manager possono appartenere ai gruppi globali sfruttando le appartenenze, indipendentemente da CA Enterprise Log Manager. L'utente può definire i gruppi dinamici e crearli attraverso un criterio di gruppo dinamico.

gruppo utenti dinamico

Un *gruppo utenti dinamico* è composto da utenti globali che condividono uno o più attributi comuni. Un gruppo utente dinamico viene creato tramite uno speciale criterio in cui il nome della risorsa è il nome del gruppo utente dinamico e l'appartenenza è basata su un set di filtri configurati in base agli attributi di utente e gruppo.

ideal_model

ideal_model è la tecnologia che esprime l'evento. Si tratta del primo campo CEG di una gerarchia di campi utilizzati per la classificazione e la normalizzazione degli eventi. Alcuni esempi di modello ideale sono gli antivirus, i DBMS, i firewall, i sistemi operativi e i server Web. I firewall Check Point, Cisco PIX e Netscreen/Juniper possono essere normalizzati con un valore di Firewall nel campo ideal_model.

identità

Un'*identità* in CA Enterprise Log Manager è un gruppo o un utente cui è consentito di accedere all'istanza applicazione di CAELM ed alle relative risorse. Un'identità per ogni prodotto CA può essere un utente globale o un utente applicazione, oppure un gruppo globale, di applicazione o dinamico.

Il NIST

Il *National Institute of Standards and Technology (NIST)*, ovvero l'Istituto nazionale degli standard e della tecnologia, è l'agenzia tecnologica federale che, nella sua pubblicazione speciale 800-92 *Guide to Computer Security Log Management (Guida alla gestione dei registri della sicurezza informatica)*, fornisce le indicazioni utilizzate come base per CA Enterprise Log Manager.

Il ruolo di amministratore

Il *ruolo di amministratore* consente agli utenti di eseguire tutte le azioni valide su ogni risorsa diCA Enterprise Log Manager. Soltanto gli amministratori possono configurare i servizi e la raccolta dei registri, o gestire gli utenti, i criteri e i filtri di accesso.

Il ruolo di analista

Il *ruolo di analista* consente agli utenti di creare e di modificare i rapporti e le query personalizzate, di modificare e di annotare i rapporti, di creare i tag e di pianificare i rapporti e gli avvisi. Gli analisti possono anche eseguire tutte le attività dei revisori.

Il ruolo di revisore

Il *ruolo di revisore* conferisce agli utenti l'accesso ai rapporti ed ai dati in essi contenuti. I revisori possono visualizzare i rapporti, l'elenco di modelli di rapporto, quello dei processi di rapporto pianificati e quello dei rapporti generati. I revisori possono anche pianificare ed annotare i rapporti. I revisori non possono accedere ai feed RSS (Rich Site Summary) a meno di impostare la configurazione in modo da non richiedere l'autenticazione per visualizzare gli avvisi.

installatore

L'*installatore* è la persona che installa l'applicazione software e gli agenti. Durante il proesso di installazione, verranno creati i nomi utente caelmadmin ed EiamAdmin, e si assegnerà a caelmadmin la password specificata per EiamAdmin. Le credenziali di caelmadmin sono necessarie per il primo accesso al sistema operativo, mentre quelle di EiamAdmin servono ad accedere per la prima volta al software CA Enterprise Log Manager e per installare gli agenti.

integrazione

L'integrazione consente di trasformare gli eventi non classificati in eventi perfezionati, in modo da poterli visualizzare nelle query e nei rapporti. È possibile implementare l'integrazione con un gruppo di elementi che consentano ad un dato agente e ad un connettore di raccogliere eventi da uno o più tipi di origini, e di inviarli a CA Enterprise Log Manager. Il gruppo di elementi comprende il sensore di registro e i file XMP e DM progettati per la lettura da un prodotto specifico. Alcuni esempi di integrazioni predefinite comprendono quelle che consentono di elaborare gli eventi syslog e WMI. È possibile creare integrazioni personalizzate per abilitare l'elaborazione degli eventi non classificati.

istanza applicazione

Una *istanza applicazione* è uno spazio comune nel repository di CA EEM in cui si memorizzano tutti i criteri, gli utenti, i gruppi, i contenuti e le configurazioni di autorizzazione. Di solito, tutti i server CA Enterprise Log Manager di un'azienda utilizzano la medesima istanza applicazione (CAELM, per impostazione predefinita). I server CA Enterprise Log Manager possono essere installati con diverse istanze applicazione, ma è possibile federare soltanto i server che condividono la medesima istanza applicazione. I server configurati per utilizzare lo stesso server CA EEM ma con diverse istanze applicazione, condividono solo l'archivio utente, i criteri di password e i gruppi globali. Diversi prodotti CA sono dotati di diverse istanze applicazione predefinite.

La grammatica evento comune (CEG, Common Event Grammar)

La Grammatica evento comune è lo schema che fornisce un formato standard in cui CA Enterprise Log Manager converte gli eventi utilizzando file di analisi e di mapping, prima di memorizzarli nell'Archivio registro eventi. La CEG utilizza campi comuni e normalizzati per definire gli eventi di protezione provenienti da diversi prodotti e piattaforme. Gli eventi impossibili da analizzare o da mappare vengono archiviati come eventi non elaborati.

libreria di analisi messaggi

La *libreria di analisi messaggi* è una libreria che riceve gli eventi dalle code dei listener e che utilizza espressioni regolari per dividere le stringhe in token, ottenendo così coppie di nomi e valori.

libreria di perfezionamento eventi

La *libreria di perfezionamento eventi* è l'archivio delle integrazioni e dei file di mapping e di analisi predefiniti o definiti dall'utente, oltre delle regole di soppressione e di riepilogo.

libreria di rapporto

La *libreria di rapporto* memorizza tutti i rapporti, i tag di rapporto, i rapporti generati e i processi di rapporto pianificati, sia predefiniti che definiti dall'utente.

libreria query

La *libreria query* memorizza tutte le query, i tag query e i filtri prompt, sia predefiniti che definiti dall'utente.

mapping dei dati

Il mapping dei dati è il processo di mapping delle coppie chiave-valore in CEG. Il mapping dei dati si esegue usando un file di mapping dei dati.

mapping di funzione

I mapping di funzione sono una parte facoltativa di un file di mapping dei dati per un'integrazione di prodotto. Il mapping di funzione si utilizza per popolare un campo CEG quando non è possibile prelevare direttamente il valore richiesto dall'evento di origine. Tutti i mapping di funzione consistono in un nome di campo CEG, in un valore di campo predefinito o di classe e nella funzione per ottenere o per calcolare il valore.

MIB

Ogni prodotto che deve ricevere avvisi da CA Enterprise Log Manager in formato di trap SNMP deve importare e compilare la *MIB (base di informazioni di gestione)* di CA Enterprise Log Manager, ovvero CA-ELM.MIB. La MIB visualizza l'origine di ogni identificatore numerico di oggetto (OID) utilizzato in un messaggio di trap SNMP con una descrizione di tale oggetto dati o elemento di rete. Nella MIB dei trap SNMP inviati da CA Enterprise Log Manager, la descrizione testuale di ogni oggetto dati si riferisce al campo CEG associato. La MIB garantisce che tutte le coppie nome/valore inviate in un trap SNMP siano interpretate in maniera corretta alla destinazione.

modulo (da scaricare)

Un *modulo* è un raggruppamento logico di aggiornamenti componente che è possibile scaricare mediante una sottoscrizione. Un modulo può contenere aggiornamenti di file binari, di contenuto o di entrambi i tipi. Ad esempio, tutti rapporti costituiscono un modulo, mentre tutti gli aggiornamenti binari dello sponsor ne costituiscono un altro. È CA a definire ciò che costituisce ogni modulo.

modulo di sottoscrizione

Un *modulo di sottoscrizione* è un servizio che consente di scaricare automaticamente dal server di sottoscrizione CA gli aggiornamenti di sottoscrizione e di distribuirli a tutti i server e agli agenti CA Enterprise Log Manager. Le impostazioni globali si applicano ai server locali di CA Enterprise Log Manager. Le impostazioni locali indicano se un server sia un proxy non in linea, in linea, oppure un client di sottoscrizione.

nome utente EiamAdmin

EiamAdmin è il nome predefinito del super utente assegnato all'installatore dei server di CA Enterprise Log Manager. Nell'installare il primo software di CA Enterprise Log Manager, l'installatore crea una password per questo account di super utente, a meno che non esista già un server remoto di CA EEM. In questo caso, l'installatore deve inserire la password esistente. Dopo aver installato l'applicazione software, l'installatore dovrà aprire un browser da una workstation, inserire l'URL di CA Enterprise Log Manager ed accedere come EiamAdmin utilizzando la password associata. Questo primo utente imposta l'archivio utente, crea i criteri di password ed il primo account utente con ruolo di amministratore. Facoltativamente, l'utente EiamAdmin può eseguire qualsiasi operazione controllata da CA EEM.

OID

Un *OID (identificatore oggetto)* è un identificatore numerico univoco di un oggetto dati accoppiato ad un valore in un messaggio di trap SNMP. Ogni OID utilizzato in un trap SNMP inviato da CA Enterprise Log Manager viene mappato su un campo CEG testuale nella MIB. Ogni OID mappato a un campo CEG ha questa sintassi: 1.3.6.1.4.1.791.9845.x.x.x, dove 791 è il numero aziendale di CA e 9845 è l'identificatore del prodotto CA Enterprise Log Manager.

origine evento

Un'*origine evento* è l'host da cui un connettore raccoglie eventi non elaborati. Un'origine evento può contenere più archivi di registro, a ognuno dei quali un connettore separato ha avuto accesso. Distribuire un nuovo connettore comporta di solito la configurazione dell'origine evento in modo che l'agente possa accedervi e leggere eventi non elaborati da uno solo dei relativi archivi di registro. Gli eventi non elaborati del sistema operativo, di diversi database e di varie applicazioni di protezione vengono memorizzati separatamente nell'origine evento.

perfezionamento eventi

Il perfezionamento eventi è il processo in cui una stringa di un evento non elaborato viene analizzata nei campi evento che la costituiscono, per poi mapparla nei campi CEG. Gli utenti possono eseguire delle query per visualizzare i dati risultanti dell'evento perfezionato. Il perfezionamento eventi segue la raccolta e precede l'archiviazione degli eventi.

plugin evento iTech

Il *plugin evento iTech* è un adapter CA che un amministratore può configurare con i file di mapping selezionati. Riceve eventi dagli iRecorder remoti, da CA EEM, dallo stesso iTechnology, o da qualsiasi prodotto che consenta di inviare eventi usando iTechnology.

pozFolder

pozFolder è un attributo di AppObject, il cui valore è il percorso padre di AppObject. L'attributo ed il valore di pozFolder vengono utilizzati nei filtri dei criteri di accesso che limitano l'accesso a risorse come rapporti, query e configurazioni.

Procedura guidata file di analisi

La *Procedura guidata file di analisi* è una funzione di CA Enterprise Log Manager che gli amministratori possono utilizzare per creare, modificare ed analizzare i file XMP (eXtensible Message Parsing) memorizzati nel server di gestione di CA Enterprise Log Manager. Per personalizzare l'analisi dei dati evento in arrivo è necessario modificare le stringhe ed i filtri di corrispondenza preliminare. I file nuovi e quelli modificati vengono visualizzati in Explorer raccolta registri, in Libreria di perfezionamento eventi, in File di analisi e nella cartella Utente.

processo di output evento/avviso

Il *processo di output evento/avviso* è il processo CA IT PAM che richiama un prodotto di terze parti per rispondere ai dati di avviso configurati in CA Enterprise Log Manager. Quando si pianifica un processo di avviso, è possibile selezionare come destinazione il Processo CA IT PAM. Quando un avviso esegue il processo CA IT PAM, CA Enterprise Log Manager invia i dati di avviso a CA IT PAM, il quale li inoltra al prodotto di terze parti con i parametri di elaborazione CA IT PAM, nell'ambito del processo di output evento/avviso.

processo valori dinamici

Un *processo di valori dinamici* è un processo CA IT PAM che è possibile selezionare per compilare o aggiornare l'elenco dei valori di una chiave selezionata utilizzata in rapporti o avvisi. Durante la configurazione di IT PAM, l'utente fornisce il percorso al Processo valori dinamici nell'Elenco del servizio dei server di rapporto, nella scheda Amministrazione. Dopodiché, l'utente fa clic sull'elenco Importa valori dinamici nella sezione Valori associata ai Valori principali sulla stessa pagina dell'interfaccia utente. Richiamare il processo valori dinamici è uno dei tre metodi che consentono di aggiungere valori alle chiavi personali.

profilo

Un *profilo* è un gruppo di tag e di filtri dati opzionale e configurabile, che può essere specifico del prodotto, della tecnologia o limitato ad una data categoria. Un filtro tag di un prodotto, ad esempio, limita i tag elencati a quelli del prodotto specificato. I filtri dati di un prodotto visualizzano, nei rapporti generati dall'utente, negli avvisi pianificati e nei risultati delle query, solo i dati per il prodotto specificato. Dopo aver creato il profilo necessario, lo si può impostare in modo che sia effettivo subito dopo aver eseguito l'accesso. Se si creano più profili, durante una sessione si potranno applicare diversi profili alle proprie attività, a patto di farlo uno per volta. I filtri predefiniti vengono distruibiti insieme agli aggiornamenti di sottoscrizione.

prompt

Un *prompt* è un tipo speciale di query che visualizza risultati in base al valore inserito ed ai campi di CEG selezionati dall'utente. Vengono restituite righe solo per gli eventi in cui il valore inserito dall'utente viene visualizzato in uno o più campi di CEG selezionati.

proxy di sottoscrizione (in linea)

Un *proxy di sottoscrizione in linea* è un CA Enterprise Log Manager con accesso ad Internet in grado di ottenere aggiornamenti di sottoscrizione da un server di sottoscrizione diCA con una pianificazione ricorrente. È possibile includere un dato proxy di sottoscrizione in linea nell'elenco dei proxy di uno o più client, che possono contattare in maniera circolare i proxy elencati per richiedere gli aggiornamenti binari. Un dato proxy online, se configurato in questo modo, invierà i nuovi contenuti e gli aggiornamenti di configurazione al server di gestione, a meno che un altro proxy non abbia già eseguito tale operazione. La directory di aggiornamento di sottoscrizione di un proxy in linea selezionato verrà utilizzata come origine per la copia degli aggiornamenti nei proxy di sottoscrizione non in linea.

proxy di sottoscrizione (non in linea)

Un *proxy di sottoscrizione non in linea* è un server CA Enterprise Log Manager che può ottenere aggiornamenti di sottoscrizione eseguendo una copia manuale di directory (usando scp) da un proxy di sottoscrizione in linea. È possibile configurare i proxy di sottoscrizione non in linea in modo da scaricare i file binari di aggiornamento sui client che li richiedono, ed inviare l'ultima versione degli aggiornamenti di contenuto al server di gestione, nel caso in cui esso non li abbia già ricevuti. I proxy di sottoscrizione non in linea non richiedono un accesso ad Internet.

proxy di sottoscrizione (per gli aggiornamenti di contenuto)

I *proxy di sottoscrizione per gli aggiornamenti di contenuto* sono i proxy di sottoscrizione scelti per aggiornare il server di gestione CA Enterprise Log Manager con gli aggiornamenti di contenuto scaricati dal server di sottoscrizione CA. È consigliabile configurare più proxy per la ridondanza.

proxy di sottoscrizione (per il client)

Il *proxy di sottoscrizione per il client* integra l'elenco di proxy di sottoscrizione che il client può contattare in maniera circolare per ottenere il software CA Enterprise Log Manager e gli aggiornamenti del sistema operativo. Se un proxy è occupato, verrà contattato il successivo nella lista. Nel caso fossero tutti occupati ed il client sia in linea, si utilizzerà il proxy di sottoscrizione predefinito.

proxy di sottoscrizione (predefinito)

Il *proxy di sottoscrizione predefinito* è di solito il server CA Enterprise Log Manager installato per primo, oppure anche il CA Enterprise Log Manager principale. Il proxy di sottoscrizione predefinito è anche un proxy di sottoscrizione in linea, e deve pertanto disporre di un accesso ad Internet. Se non si definiscono altri proxy di sottoscrizione, tale server otterrà gli aggiornamenti di sottoscrizione dal server di sottoscrizione CA e scaricherà gli aggiornamenti binari su tutti i client, per poi inviare ad CA EEM gli aggiornamenti di contenuto. Se si definiscono altri proxy, tale server riceverà ugualmente gli aggiornamenti di sottoscrizione. I client per gli aggiornamenti, però, lo contatteranno solo quando non verrà configurato nessun elenco di proxy di sottoscrizione, o quando tale elenco sarà esaurito.

punto di raccolta

Un *punto di raccolta* è un server su cui si installa un agente, dotato di prossimità di rete con tutti i server che dispongono di origini evento associate ai connettori del proprio agente.

query

Una *query* è un gruppo di criteri utilizzato per cercare negli archivi registro evento del server CA Enterprise Log Manager attivo e, se specificati, nei suoi server federati. Una query agisce sui database hot, warm o defrosted specificati nella sua clausola Dove. Per esempio, se la clausola Dove limita la query agli eventi con source_username="myname" in un determinato intervallo di tempo, e se solo 10 dei 1000 database contengono record corrispondenti a questo criterio in base alle informazioni nel database di catalogo, la query agirà solo su questi dieci database. Una query può produrre un massimo di 5000 righe di dati. Qualsiasi utente con un ruolo predefinito può eseguire una query. Solo gli analisti e gli amministratori possono pianificare una query per distribuire un avviso, per creare un rapporto selezionando le query da inserire o per creare una query personalizzata utilizzando la procedura guidata Progettazione query. Consultare anche Archivia query.

query azione

Una *query azione* è una query che supporta un avviso. Si esegue con pianificazione ricorrente allo scopo di verificare le condizioni delineate dall'avviso cui essa è allegata.

query di archiviazione

Una *query di archiviazione* è una query del catalogo utile per identificare i database cold che necessitino di un ripristino e di un defrost per poter eseguire una query. Una query di archiviazione differisce da una normale. Essa agisce infatti sui database cold, mentre una query normale agisce sui database hot, warm e defrosted. Gli amministratori possono eseguire una query di archiviazione dalla scheda Amministrazione, sottoscheda Raccolta registri, opzione Archivia query di catalogo.

raccolta eventi

La raccolta eventi è il processo di lettura delle stringhe degli eventi non elaborati da un'origine evento, per poi inviarli al CA Enterprise Log Manager configurato. Il perfezionamento eventi avverrà dopo la raccolta di eventi.

raccolta registri diretta

La raccolta registri diretta è la tecnica di raccolta dei registri in cui non esiste alcun agente intermedio fra l'origine evento ed il software CA Enterprise Log Manager.

Rapporti relativi ad EPHI

I *rapporti relativi a EPHI* sono rapporti incentrati sulla protezione HIPAA, in cui EPHI significa Informazioni sanitarie elettroniche protette (Electronic Protected Health Information). Tali rapporti consentono di dimostrare la protezione della creazione, della manutenzione e della trasmissione elettronica di tutte le informazioni sanitarie singolarmente identificabili e correlate ai pazienti.

rapporto

Un *rapporto* è una visualizzazione grafica o tabulare dei dati del registro eventi generata eseguendo query predefinite o personalizzate con filtri. I dati provengono da database hot, warm o defrosted dell'archivio registro eventi del server selezionato e, se richiesto, dei server federati.

record di controllo

I record di controllo contengono eventi di protezione come i tentativi di autenticazione, gli accessi ai file e le modifiche ai criteri di protezione, agli account utente o ai privilegi. Gli amministratori possono specificare quale tipo di evento controllare e quale inserire nei registri.

record di registro

Un *record di registro* è un singolo record di controllo.

registro

Un *registro* è un record di controllo, o messaggio registrato, di un evento o di una raccolta di eventi. Un registro può essere di controllo, di transazione, di intrusione, di connessione, di prestazioni di sistema, di attività utente o di avviso.

regole di riepilogo

Le regole di riepilogo sono regole che uniscono alcuni eventi nativi di tipo comune ottenendo così un unico evento perfezionato. Ad esempio, è possibile configurare una regola di riepilogo per sostituire fino a 1000 eventi duplicati, con gli stessi indirizzi IP e porte di origine e di destinazione, con un singolo evento di riepilogo. Regole di questo tipo semplificano l'analisi degli eventi e riducono il traffico di registro.

regole di soppressione

Le regole di soppressione sono delle regole da configurare per impedire ad alcuni eventi perfezionati di apparire nei propri rapporti. È possibile creare regole di soppressione permanenti per eliminare gli eventi di routine che non riguardano la protezione, oltre a creare regole temporanee per eliminare la registrazione di eventi pianificati come la creazione di molti nuovi utenti.

regole inoltro eventi

Le regole *inoltro eventi* indicano che gli eventi selezionati sono da inoltrare a prodotti di terze parti, ad esempio i prodotti che stabiliscono la correlazione tra eventi, una volta salvati nell'archivio di registro eventi.

ricatalogazione

Una *ricatalogazione* è la ricostruzione forzata del catalogo. Si deve eseguire una ricatalogazione solo quando si ripristinano dei dati di un archivio registro eventi su un server diverso da quello in cui è stato generato. Ad esempio, se si sceglie un CA Enterprise Log Manager che agisca come punto di ripristino per le analisi sui dati cold, si potrebbe dover forzare una ricatalogazione del database dopo averlo ripristinato nel punto di ripristino scelto. Se necessario, la ricatalogazione si avvierà automaticamente al riavvio di iGateway. La ricatalogazione di un singolo file di database può impiegare anche diverse ore.

risorsa applicazione

Una *risorsa applicazione* è una delle risorse specifiche di CA Enterprise Log Manager per cui i criteri di accesso di CALM consentono o negano alle identità specificate di eseguire azioni specifiche dell'applicazione come creare, pianificare e modificare. Alcuni esempi di risorse applicazione sono il rapporto, l'avviso e l'integrazione. Consultare anche Risorsa globale.

risorsa globale

Una *risorsa globale* del prodotto CA Enterprise Log Manager è una risorsa condivisa con altre applicazioni CA. È possibile creare criteri di scoping con risorse globali. Alcuni esempi sono l'utente, il criterio ed il calendario. Consultare anche Risorsa applicazione.

ruolo utente

Un *ruolo utente* può essere un gruppo applicazione predefinito o un gruppo applicazione definito dall'utente. Sono necessari ruoli utente personalizzati quando i gruppi applicazione predefiniti (amministratore, analista e revisore) non sono sufficientemente dettagliati per riflettere le assegnazioni del lavoro. I ruoli utente personalizzati richiedono criteri di accesso personalizzati e la modifica dei criteri predefiniti per includere il nuovo ruolo.

SafeObject

SafeObject è una classe di risorsa predefinita di CA EEM. È la classe di risorsa memorizzata sotto l'ambito di Applicazione, ed a cui appartiene AppObjects. Gli utenti che definiscono criteri e filtri per consentire l'accesso ad AppObjects fanno riferimento a questa classe di risorse.

SAPI collector

SAPI collector è un adapter CA che consente di ricevere eventi dai client di CA Audit. I client di CA Audit inviano tramite l'azione Raccoglitore, che fornisce un failover integrato. Gli amministratori configurano CA Audit SAPI Collector con, ad esempio, le crittografie ed i file di mapping dei dati selezionati.

SAPI recorder

Il *SAPI recorder* era la tecnologia utilizzata per inviare informazioni a CA Audit prima di iTechnology. SAPI significa Submit API (Inviare interfaccia di programmazione di applicazione, Submit Application Programming Interface). I recorder di CA Audit per CA ACF2, CA Top Secret, RACF, Oracle, Sybase e DB2 sono esempi di SAPI recorder.

SAPI router

Il *SAPI router* è un adapter CA in grado di ricevere eventi dalle integrazioni, come Mainframe, per poi inviarle ad un router di CA Audit.

sensore di registro

Un *sensore di registro* è un componente di integrazione progettato per leggere un tipo specifico di registro, come database, syslog, file o SNMP. I sensori di registro possono essere riutilizzati. Di solito, gli utenti non creano sensori di registro personalizzati.

server avvisi

Il *server avvisi* è l'archivio degli avvisi e dei relativi processi.

server del punto di ripristino

Un *server del punto di ripristino* è un ruolo ricoperto da un server CA Enterprise Log Manager. Per analizzare gli eventi "cold", è possibile usare un'utility per spostare i database dal server di archiviazione remota a quello del punto di ripristino, per poi aggiungerli al catalogo ed eseguire delle query. Lo spostamento dei database cold in un punto di ripristino dedicato è un'alternativa al riportarli nel server di rapporto originale in modo da poter eseguire delle analisi.

server di archiviazione remota

Un *server di archiviazione remota* è un ruolo assegnato ad un server che riceva i database archiviati automaticamente da uno o più server di rapporto. Un server di archiviazione remota memorizza i database cold per il numero di anni necessari. Di solito non conviene installare CA Enterprise Log Manager, o altri prodotti, negli host remoti per la memorizzazione. Per l'archiviazione automatica, configurare l'autenticazione non interattiva.

server di federazione

I server di federazione sono server CA Enterprise Log Manager collegati l'un l'altro nella rete per distribuire la raccolta dei dati di registro, ma aggregando i dati raccolti in modo da creare un rapporto. I server di federazione possono essere collegati tramite una topologia gerarchica o a coppie. I rapporti dei dati federati comprendono quelli provenienti dal server di destinazione, oltre a quelli provenienti dai figli o dai peer di tale server, se presenti.

server di gestione

Il *server di gestione* è un ruolo assegnato al primo server CA Enterprise Log Manager installato. Questo server CA Enterprise Log Manager contiene il repository che contiene i contenuti condivisi per tutti i CA Enterprise Log Manager, come ad esempio i criteri. Tale server è di solito il proxy predefinito di sottoscrizione. Il server di gestione può ricoprire tutti i ruoli, anche se si tratta di una pratica sconsigliata per la maggior parte degli ambienti di produzione.

server di raccolta

Un *server di raccolta* è un ruolo ricoperto da un server CA Enterprise Log Manager. Il server di raccolta rifinisce i registri evento in arrivo e li inserisce nel database hot. Fatto ciò, comprime ed archivia automaticamente, o copia, tale database nel server di rapporto correlato. Il server di raccolta comprime il database hot quando esso raggiunge le dimensioni configurate, e lo archivia automaticamente seguendo la pianificazione configurata.

server di rapporto

Un *server di rapporto* è un ruolo ricoperto da un server CA Enterprise Log Manager. Un server di rapporto riceve database warm archiviati automaticamente da uno o più server di raccolta. Un server di rapporto può gestire query, rapporti, avvisi e rapporti pianificati.

server di rapporto

Il *server di rapporto* è il servizio che archivia informazioni di configurazione come il server da utilizzare nell'inviare gli avvisi via posta elettronica, l'aspetto visivo dei rapporti salvati in formato PDF, la memorizzazione dei criteri per i rapporti salvati nel server di rapporto e gli avvisi inviati al feed RSS.

server di sottoscrizione CA

Il *server di sottoscrizione CA* è l'origine degli aggiornamenti di sottoscrizione da CA.

Server ODBC

Il *server ODBC* è il servizio configurato che imposta la porta utilizzata per le comunicazioni tra il client ODBC o JDBC e il server CA Enterprise Log Manager e specifica se utilizzare la crittografia SSL.

server proxy HTTP

Un *server proxy HTTP* è un server proxy in grado di agire come firewall, impedendo al traffico Internet di entrare o uscire dall'azienda se non attraverso il proxy. Il traffico in uscita può specificare un ID e una password che consentano di bypassare il server proxy. È possibile configurare l'utilizzo di un server proxy HTTP locale nella gestione delle sottoscrizioni.

servizi

I *servizi* CA Enterprise Log Manager sono l'archivio registro eventi, il server di rapporto e la sottoscrizione. Gli amministratori possono configurare tali servizi a livello globale dove, per impostazione predefinita, tutte le impostazioni si applichino ad ogni CA Enterprise Log Manager. La maggior parte delle impostazioni globali per i servizi si possono ignorare a livello locale, ovvero per ogni CA Enterprise Log Manager specificato.

SNMP

SNMP è l'acronimo di protocollo di gestione di rete semplice (Simple Network Management Protocol), uno standard aperto per l'invio di messaggi di avviso sottoforma di trap SNMP da un sistema di agente ad uno o più sistemi di gestione.

soppressione

La soppressione è il processo di rimozione degli eventi in base ai filtri di CEG. La soppressione si esegue usando file SUP.

stati del database

Gli *stati del database* sono i seguenti: hot, per i database non compressi costituiti da nuovi eventi; warm, per un database di eventi compressi; cold, per un database sottoposto a backup; defrosted, per un database ripristinato nell'archivio registro eventi da cui è stato eseguito il backup. È possibile eseguire query sia su database hot che warm e defrosted. Una query di archiviazione visualizza informazioni sui database cold.

stato di database cold

Lo *stato di database cold* si applica ad un database warm quando un amministratore esegue LMArchive per avvertire CA Enterprise Log Manager dell'avvenuta esecuzione di un backup del database. Gli amministratori devono eseguire i backup dei database warm, ed eseguire questa utility prima della loro eliminazione. Un database warm verrà automaticamente cancellato quando la sua età supererà il valore indicato in Numero massimo di giorni di archiviazione, oppure quando si raggiungerà la soglia dello Spazio su disco di archiviazione, indipendentemente da quale dei due si verifichi prima. È possibile eseguire una query sul database di archiviazione per identificare i database con stato warm e cold.

stato di database defrosted

Uno *stato di database defrosted* è quello applicato ad un database ripristinato nella directory di archiviazione dopo che l'amministratore ha eseguito l'utility LMArchive per avvisare CA Enterprise Log Manager dell'avvenuto ripristino. I database defrosted si conservano per il numero di ore configurate in Criterio di esportazione. È possibile eseguire una query di registri evento nei database di stato hot, warm e defrosted.

stato di database hot

Uno *stato di database hot* è lo stato di un database dell'archivio registro eventi nel momento in cui si inseriscono nuovi eventi. Quando il database hot raggiunge dimensioni configurabili sul server di raccolta, lo si comprime, cataloga e trasferisce in un archivio warm sul server di rapporto. Inoltre, tutti i server memorizzano i nuovi eventi di automonitoraggio in un database hot.

stato warm del database

Lo *stato warm del database* è quello in cui un database hot di registri evento si evolve quando si superano le dimensioni (Numero massimo di righe) di quest'ultimo, oppure quando si esegue una ricatalogazione dopo il ripristino di un database cold in un nuovo archivio registro eventi. I database warm vengono compressi e conservati nell'archivio registro eventi fino a quando la loro età in giorni supera il valore configurato per Numero massimo di giorni di archiviazione. È possibile eseguire una query di registri evento nei database di stato hot, warm e defrosted.

tag

Un *tag* è un termine o una frase chiave utilizzata per identificare i rapporti o le query che appartengono allo stesso gruppo relativo ai business. I tag consentono di eseguire ricerche basate sui gruppi relativi ai business. Tag è anche il nome di risorsa utilizzato in qualsiasi criterio che consenta agli utenti di creare un tag.

token di analisi del messaggio (ELM)

Un *token di analisi del messaggio* è un modello riutilizzabile per costruire la sintassi dell'espressione regolare utilizzata da CA Enterprise Log Manager per l'analisi del messaggio. Un token possiede un nome, un tipo ed una stringa della corrispondente espressione regolare.

URL del feed RSS per gli avvisi

L'*URL del feed RSS per gli avvisi* è: https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp. Da questo URL è possibile visualizzare gli avvisi sulle azioni soggetti alla configurazione di età e quantità massime.

URL del feed RSS per la sottoscrizione

L'*URL del feed RSS per la sottoscrizione* è un collegamento preconfigurato utilizzato dai server proxy di sottoscrizione in linea per recuperare gli aggiornamenti di sottoscrizione. Questo URL vale per il server di sottoscrizione CA.

URL di CA Embedded Entitlements Manager

L'*URL di CA Embedded Entitlements Manager* (CA EEM) è: https://<ip_address>:5250/spin/eiam. Per accedere, selezionare CAELM come applicazione ed inserire la password associata al nome utente EiamAdmin.

URL di CA Enterprise Log Manager

L'*URL di CA Enterprise Log Manager* è: https://<ip_address>:5250/spin/calm. Per accedere, inserire il nome utente del proprio account definito dall'amministratore e la password associata. Oppure, inserire il nome predefinito del super utente EiamAdmin e la password associata.

utente applicazione

Un *utente applicazione* è un utente globale a cui si assegnano dettagli a livello di applicazione I dettagli utente dell'applicazione CA Enterprise Log Manager comprendono il gruppo utente e qualsiasi restrizione di accesso. Se l'archivio utente è il repository locale, i dettagli utente dell'applicazione conterranno anche le credenziali di accesso e criteri di password.

Utente EEM

L'*Utente EEM*, configurato nella sezione di archiviazione automatica dell'archivio registro eventi, indica l'utente che può eseguire una query di archiviazione, ricatalogare il database di archivio ed eseguire l'utility LMArchive e lo script shell restore-ca-elm per ripristinare i database d'archiviazione in modo da poterli analizzare. Si deve assegnare a tale utente il ruolo predefinito di amministratore, oppure uno personalizzato associato ad un criterio personalizzato che consenta l'azione di modifica sulla risorsa Database.

utente globale

Un *utente globale* è l'informazione dell'account utente che esclude i dettagli specifici dell'applicazione. I dettagli dell'utente globale e le appartenenze al gruppo globale sono condivisi in tutte le applicazioni CA che si integrano con l'archivio utente predefinito. È possibile memorizzare i dettagli dell'utente globale nel repository integrato oppure in una directory esterna.

utility LMArchive

L'*utility LMArchive* si esegue dalla linea di comando, e tiene traccia del procedimento di backup e di ripristino dei database di archivio nell'archivio registro eventi di un server CA Enterprise Log Manager. Utilizzare LMArchive per eseguire una query utile per ottenere l'elenco dei database warm pronti per l'archiviazione. Dopo aver eseguito il backup del database elencato ed averlo spostato nell'archivio a lungo termine (cold), utilizzare LMArchive per creare un record su CA Enterprise Log Manager che indichi l'avvenuta esecuzione del backup di questo database. Dopo l'avvenuto ripristino di un database cold nel suo CA Enterprise Log Manager originale, utilizzare LMArchive per inviare una notifica a CA Enterprise Log Manager, che a sua volta trasformerà i file del database in stato defrosted, in modo da poter ricevere delle query.

utility LMSEOSImport

L'*utility LMSEOSImport* è un'utility da riga di comando e consente di importare SEOSDATA o eventi esistenti in CA Enterprise Log Manager, durante la migrazione da Audit Reporter, da Viewer o da Audit Collector. Solo Microsoft Windows e Sun Solaris Sparc supportano questa utility.

utility scp

L'utility *scp*, copia sicura, (un programma di copia di file remoti) è un'utility UNIX che consente di trasferire file fra i diversi computer UNIX in una rete. È possibile utilizzare questa utility subito dopo l'installazione di CA Enterprise Log Manager, per trasferire i file di aggiornamento di sottoscrizione dal proxy di sottoscrizione in linea a quello non in linea.

valori principali

I valori principali sono valori definiti dell'utente ed assegnati a un elenco anch'esso definito dall'utente (gruppo principale). Quando una query utilizza un gruppo principale, i risultati della ricerca contengono le corrispondenze a qualsiasi valore principale presente nel gruppo principale. Esistono diversi gruppi principali predefiniti utilizzati nelle query e nei rapporti predefiniti. Alcuni gruppi contengono valori principali predefiniti.

voce di registro

Una *voce di registro* è una voce in un registro contenente informazioni su un evento specifico verificatosi nel sistema o in una rete.

Indice