CA User Activity Reporting Module

Guida generale

Versione 12.5.03

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 User Activity Reporting Module.
- 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 User Activity Reporting Module.

Ulteriori informazioni:

Panoramica di avvio rapido (a pagina 13)
Avviso di violazione del criterio (a pagina 57)
Esplorazione della Bookshelf della documentazione (a pagina 68)

Sommario

Capitolo 1: Introduzione

Questa sezione contiene i seguenti argomenti:

Informazioni sulla guida

In questa *Guida generale* viene presentato CA User Activity Reporting Module. 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 User Activity Reporting Module 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 User Activity Reporting Module	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 User Activity Reporting Module 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 User Activity Reporting Module, consultare la guida in linea.

Informazioni su CA User Activity Reporting Module

CA User Activity Reporting Module 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.

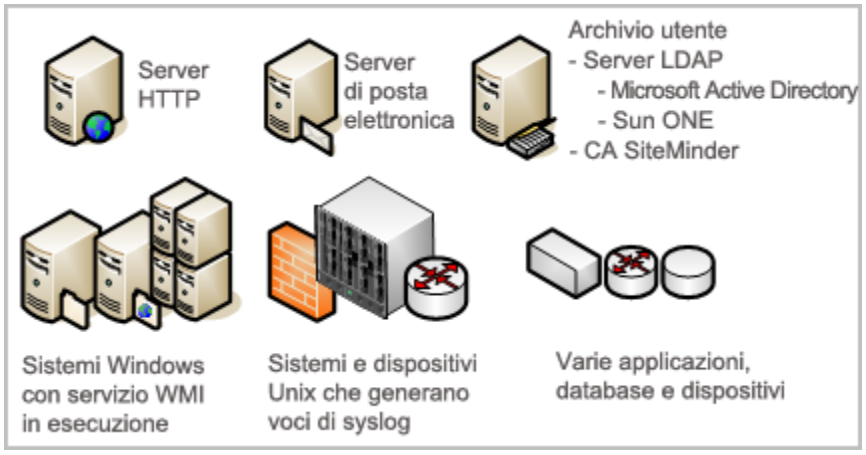
Rete dell'utente-Prima dell'installazione

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 User Activity Reporting Module offre questi vantaggi e, in caso di eventi critici, consente di inviare avvisi a singole persone ed a sistemi.

Elementi da installare

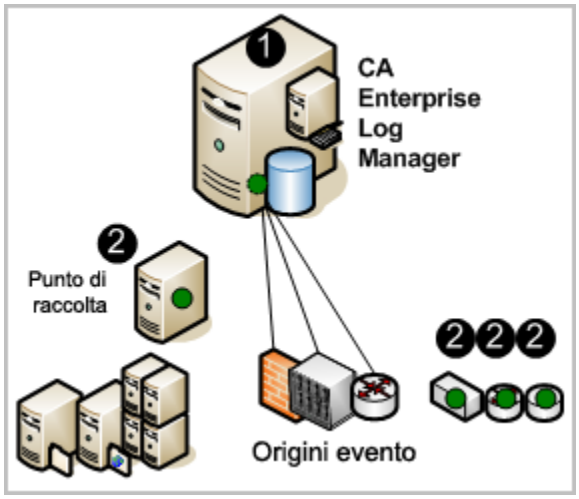
Non occorre molto tempo per configurare una soluzione a server singolo e iniziare a raccogliere eventi.

I dischi di installazione includono i seguenti componenti:

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

Nella figura seguente, CA User Activity Reporting Module 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 User Activity Reporting Module. Non appena le origini vengono configurate per l'invio dei syslog a CA User Activity Reporting Module 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 40)

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 User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module.

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 User Activity Reporting Module 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

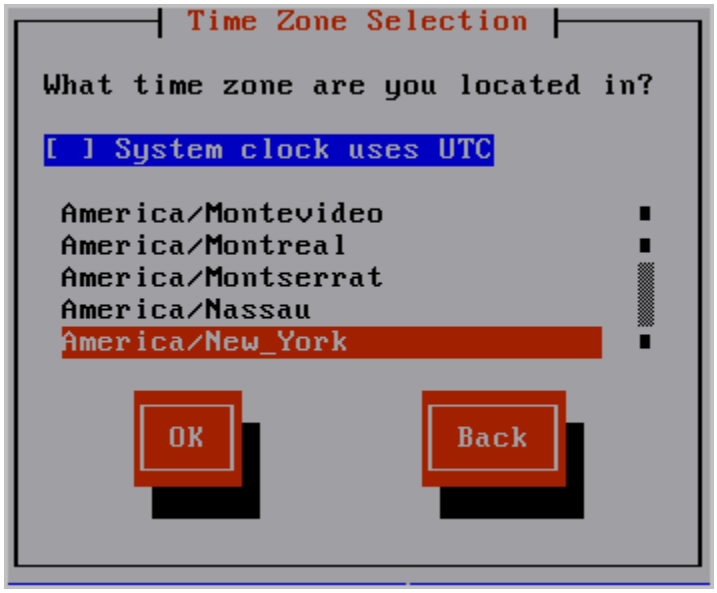
     Nota: il dominio deve essere registrato con i server DNS sulla propria rete per completare l'installazione.
   - Indirizzi IP dei server DNS
   - (Facoltativo) Indirizzo IP del server con orario NTP
   - Una password per il nome del super utente per l'installazione predefinito, EiamAdmin
   - CAELM.

     È il nome dell'applicazione predefinita per l'applicazione CA User Activity Reporting Module.

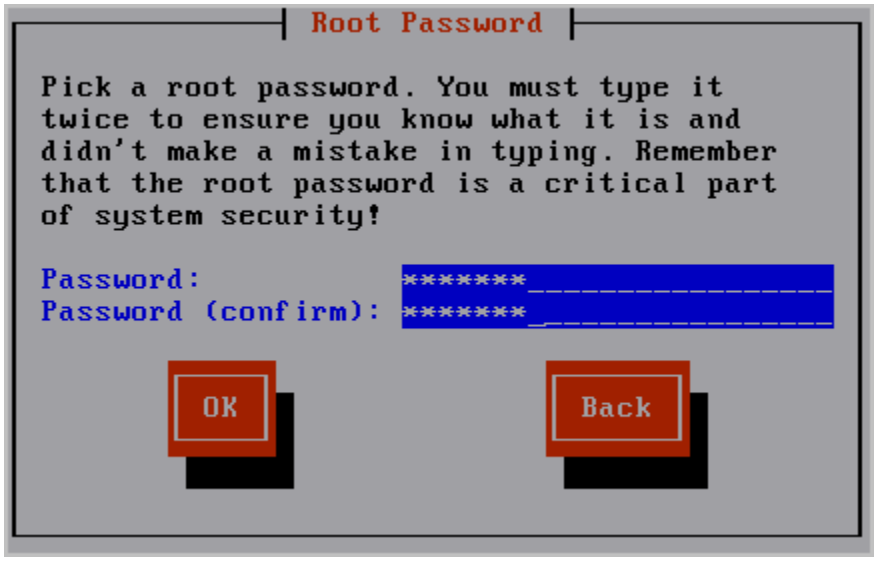
2. Installare il sistema operativo preconfigurato utilizzando il supporto creato per il pacchetto di download di CA User Activity Reporting Module. Durante l'installazione del sistema operativo, eseguire le seguenti procedure:

   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 User Activity Reporting Module. Premere Invio.

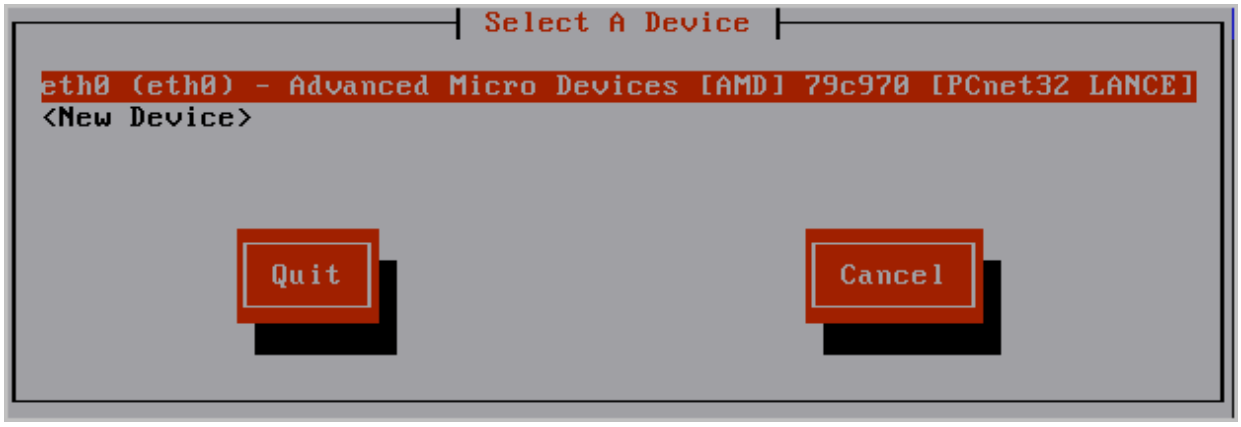
   Il sistema viene riesaminato per vedere se soddisfa le specifiche minime consigliate per ottenere prestazioni ottimali. In caso contrario, viene visualizzato un prompt che chiede se si desidera interrompere il processo di installazione.

   Verrà visualizzato il seguente prompt:

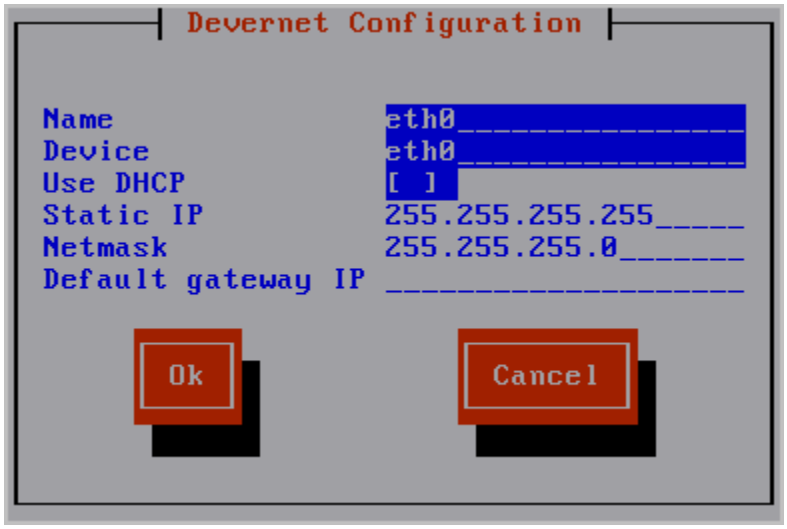
   ```
   Immettere un nuovo nome host:
   ```

4. Immettere il nome host per questa applicazione software CA User Activity Reporting Module. 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 User Activity Reporting Module 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.

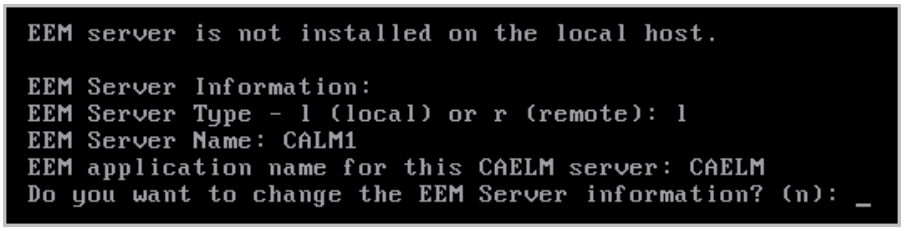
       ```
       Immettere la password per l'utente EiamAdmin del server EEM:
       Confermare la password per l'utente EiamAdmin del server EEM:
       ```

    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 User Activity Reporting Module.

   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 User Activity Reporting Module, 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 User Activity Reporting Module 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 User Activity Reporting Module. 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 User Activity Reporting Module, 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 User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module, predisporre la configurazione andando all'URL di CA User Activity Reporting Module 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 User Activity Reporting Module.

   `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 User Activity Reporting Module.

   c. Fare clic su Sì.

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

   d. Fare clic su OK.

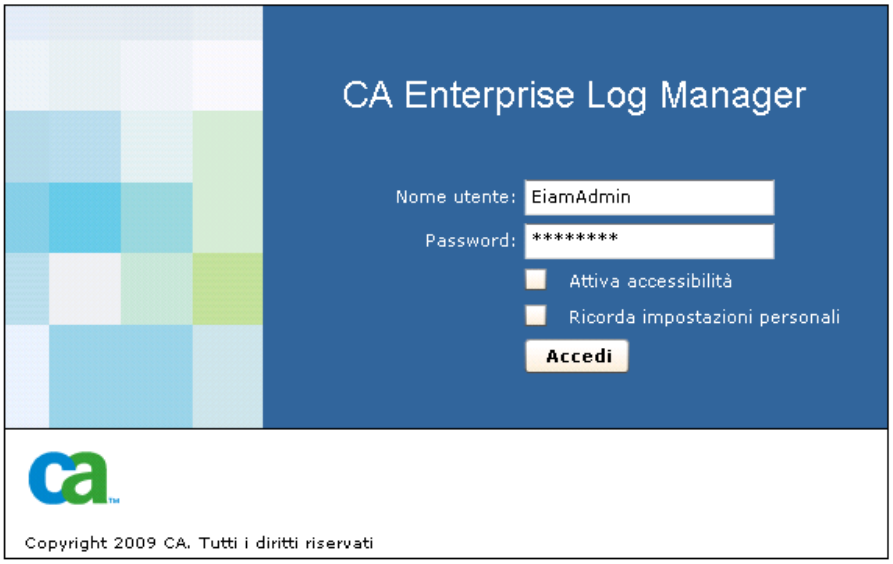
      Viene visualizzata la finestra di dialogo Certificati attendibili.

   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.

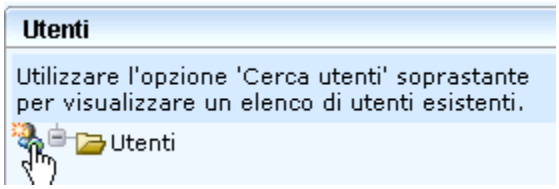
3. Accedere con il nome utente EiamAdmin e la password creata al momento dell'installazione del software. Fare clic su Accedi.



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

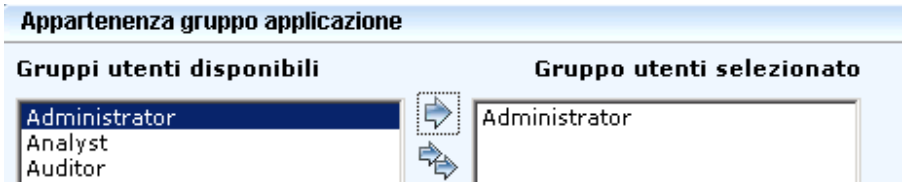
4. Fare clic su Utenti.

5. Fare clic su Aggiungi nuovo utente.

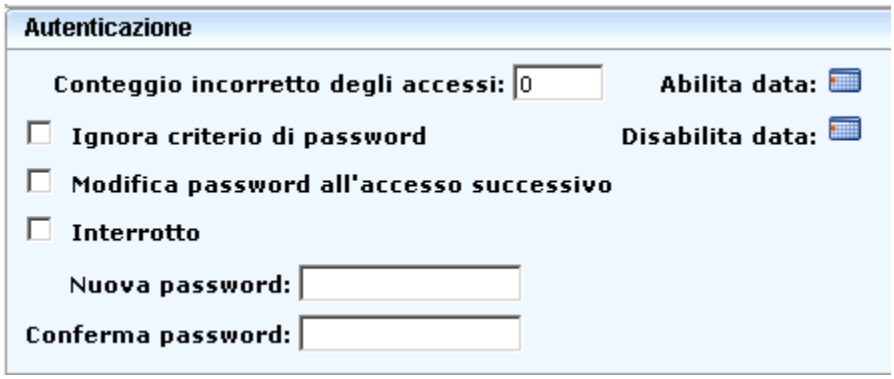


6. Inserire il proprio nome nel campo Nome e fare clic su Aggiungi dettagli utente applicazione.

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 User Activity Reporting Module con le credenziali di amministratore appena definite.

    CA User Activity Reporting Module 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 User Activity Reporting Module, 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 User Activity Reporting Module 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.

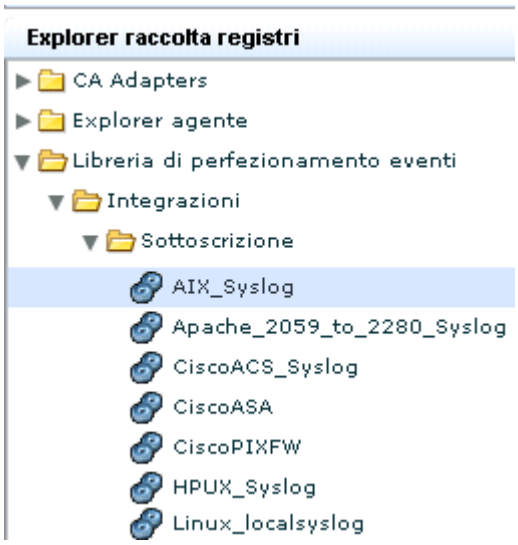
Configurare l'origine di un evento syslog selezionato

1. Accedere all'host con un'origine evento syslog di destinazione.
2. Avviare CA User Activity Reporting Module 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.

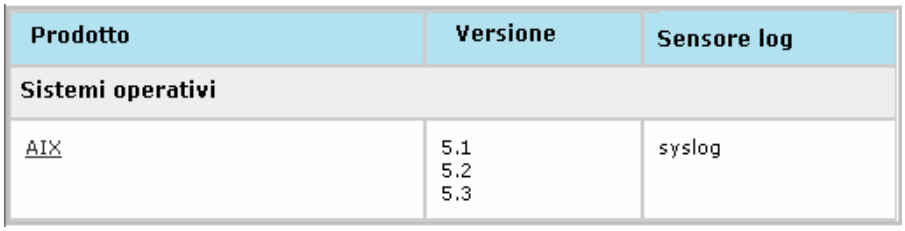
   Viene visualizzata la guida al connettore per l'integrazione selezionata.

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 User Activity Reporting Module.

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

È possibile aprire una guida al connettore selezionata dall'interno dell'interfaccia utente CA User Activity Reporting Module 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 User Activity Reporting Module dispone di un agente predefinito. Quando si installa un CA User Activity Reporting Module , 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 User Activity Reporting Module. Tuttavia, perché CA User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module.

3. Selezionare il nome di un server CA User Activity Reporting Module.

   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.

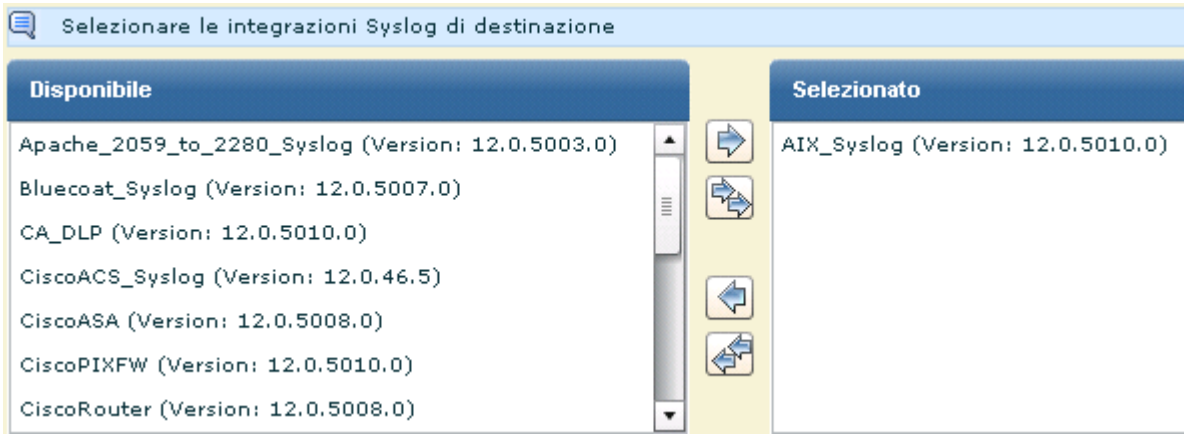
5. (Facoltativo) Fare clic su Applica regole di soppressione. Se si desidera sopprimere, ovvero *non* raccogliere, un evento syslog qualunque, spostare il tipo di evento dall'elenco disponibile a quello selezionato. Selezionare l'evento da spostare e fare clic sul pulsante corrispondente all'azione.

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 User Activity Reporting Module. 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.

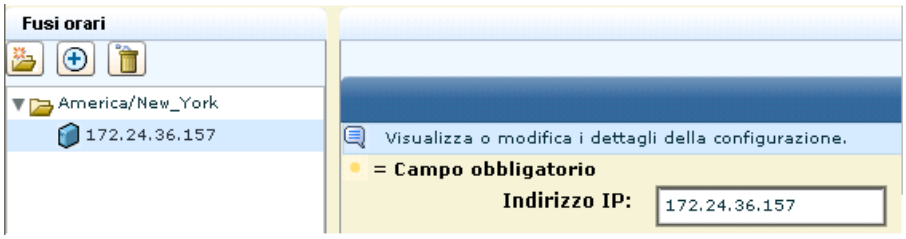
   Generalmente, è possibile accettare le porte UPD e TCP predefinite per l'agente predefinito.

   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.

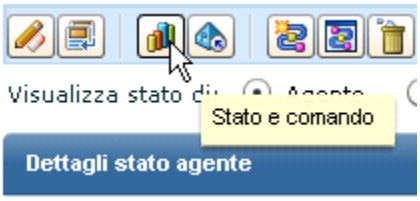
    b. Selezionare la voce vuota sotto la cartella. Inserire l'indirizzo IP di un host attendibile configurato per questo connettore o del server di riferimento orario NTP specificato al momento dell'installazione del CA User Activity Reporting Module.



11. Fare clic su Salva e chiudi.

12. Visualizzare lo stato.

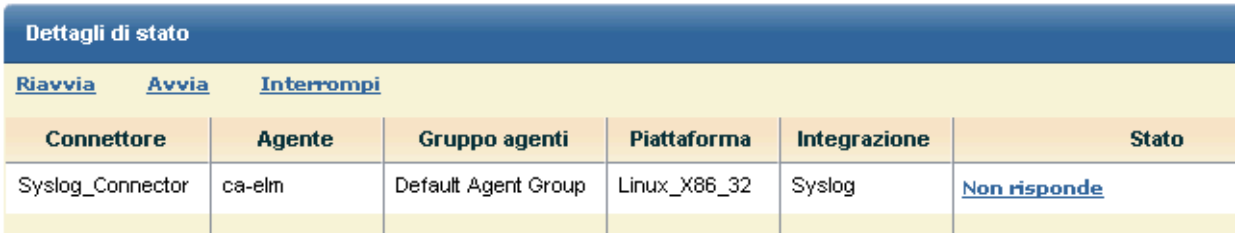
    a. Fare clic su Stato e comando.



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

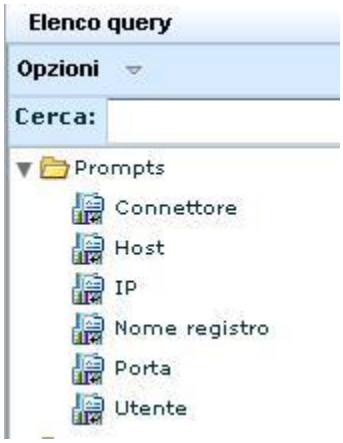
Uno dei modi più veloci per visualizzare i risultati delle query sugli eventi raccolti da un listener di syslog consiste nell'utilizzo del prompt per host.

Per visualizzare gli eventi syslog

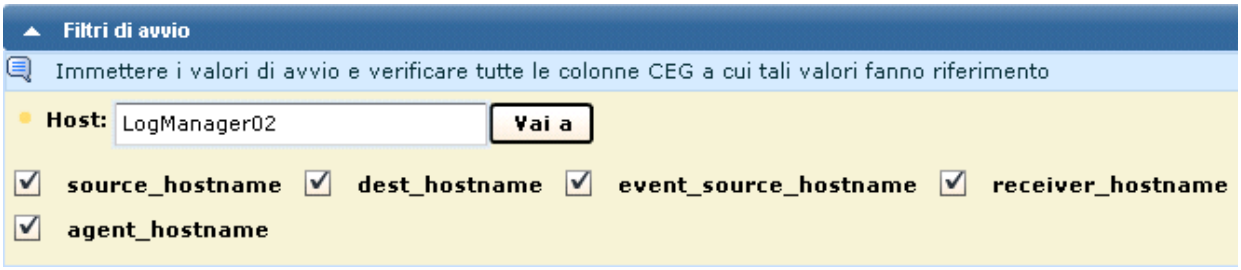
1. Selezionare la scheda Query e rapporti.

   Viene visualizzata la sottoscheda Query.

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



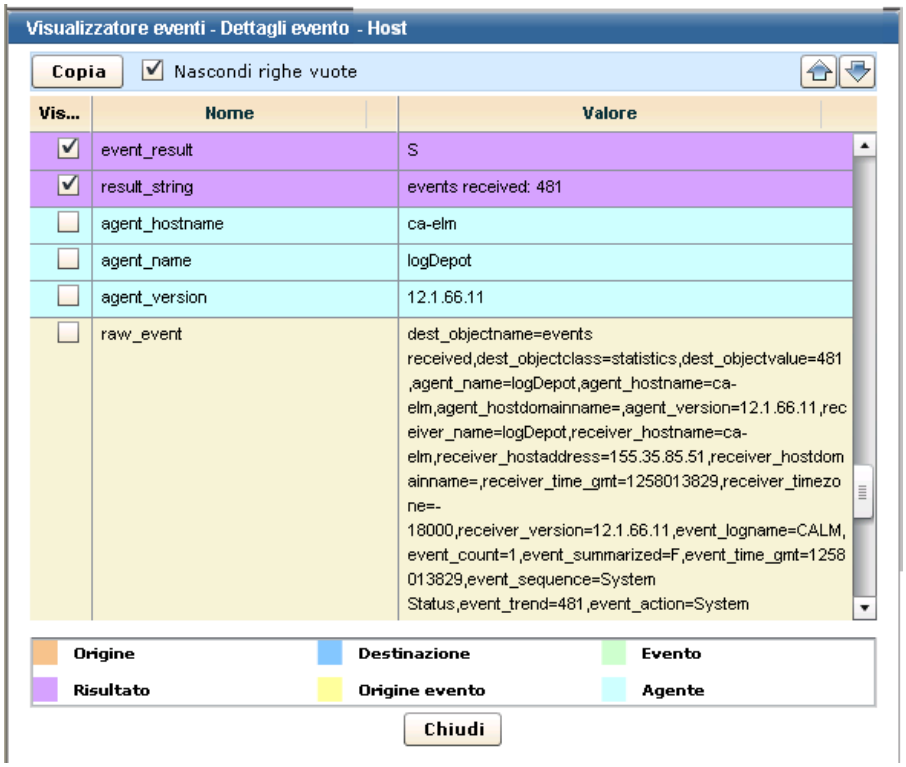
3. Inviare una query per gli eventi raccolti dall'agente predefinito.
   a. Immettere il nome host dell'agente predefinito nel campo Host, che corrisponde al nome del CA User Activity Reporting Module su cui esso risiede.
   b. Selezionare agent_hostname.
   c. Fare clic su Vai a.



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 User Activity Reporting Module 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.

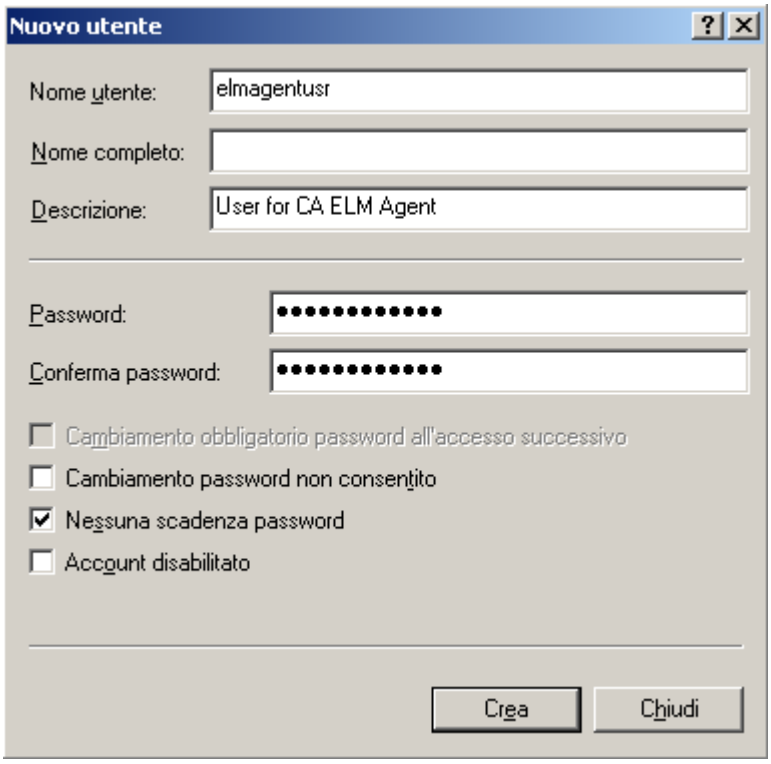
Nota: è possibile saltare questo passaggio e specificare le credenziali di dominio di un Amministratore per l'agente nel momento in cui si esegue l'installazione, ma non è considerata una buona prassi.

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 40)

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 User Activity Reporting Module per questo agente. Di seguito un esempio:

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

2. Accedere al server CA User Activity Reporting Module. 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.

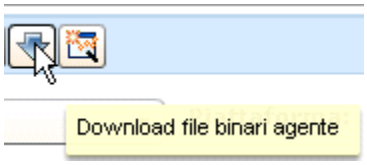
7. Fare clic su Salva.
8. Proseguire con il passaggio successivo, Download del programma di installazione dell'agente.

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.

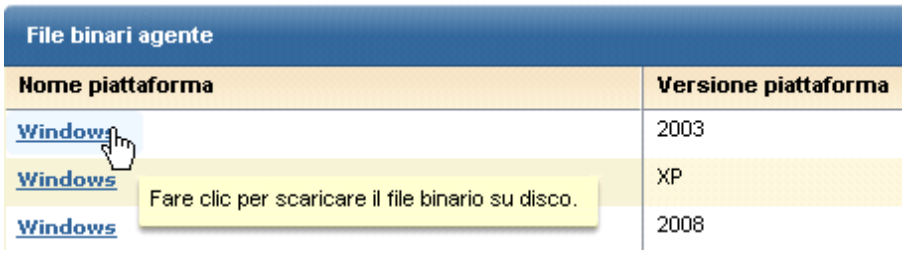
Per scaricare il programma di installazione dell'agente

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.



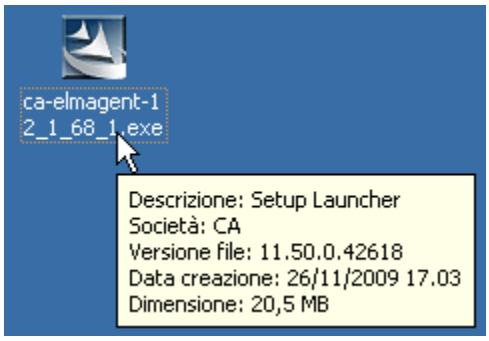
Viene visualizzata la finestra di dialogo Seleziona posizione per il download in base a <indirizzo IP>.

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 User Activity Reporting Module 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.

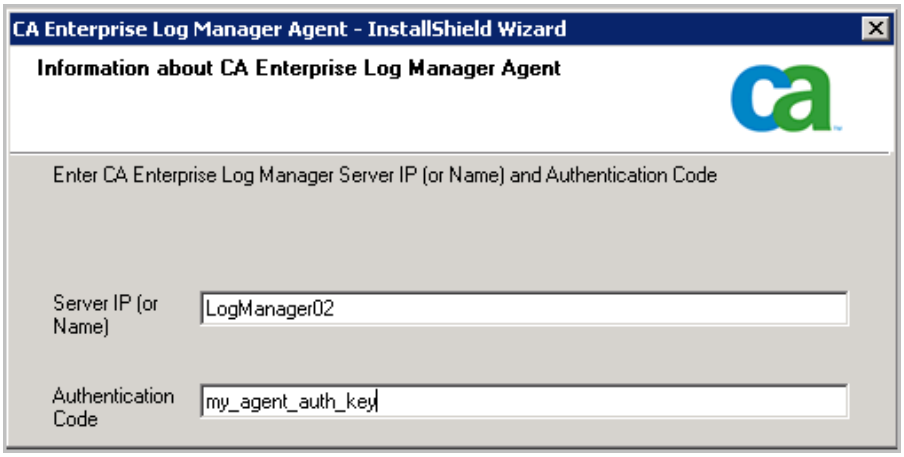
4. Immettere le informazioni richieste nel modo seguente:

   a. Inserire il nome host del CA User Activity Reporting Module a cui questo agente deve inoltrare i registri che raccoglie.

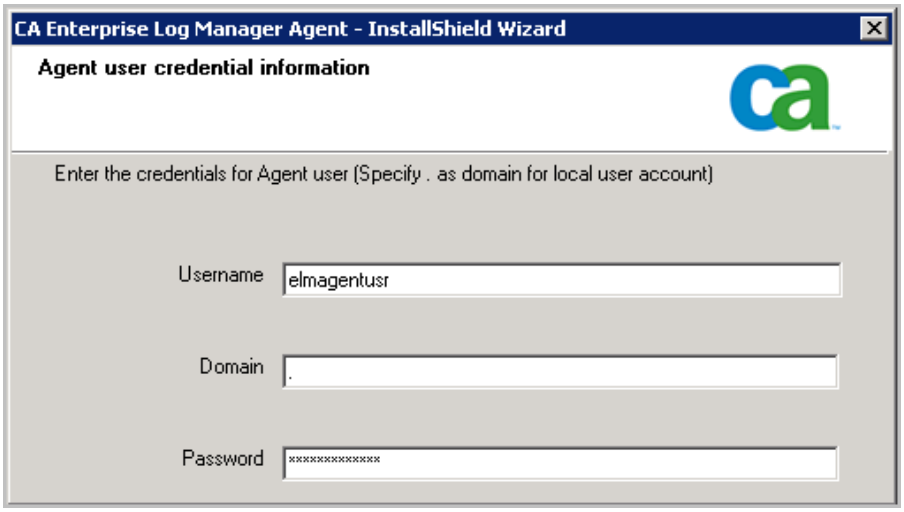
      Nota: dato che in questo scenario di esempio il CA User Activity Reporting Module utilizza DHCP per l'assegnazione dell'indirizzo IP, quest'ultimo non dovrebbe essere inserito. Inserendolo, si correrebbe il rischio di dover reinstallare l'agente se l'indirizzo IP del server dovesse cambiare.

   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 User Activity Reporting Module 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 39)
Creare un account utente per l'agente (a pagina 36)
Impostare la chiave di autenticazione agente. (a pagina 38)

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.

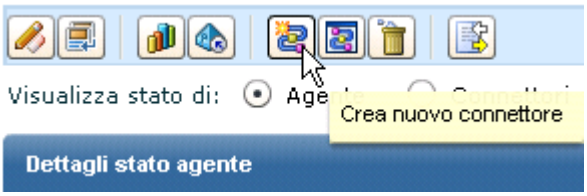
Per configurare un connettore basato su NTEventLog

1. Ingrandire il browser che visualizza l'Explorer agente di CA User Activity Reporting Module.
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.

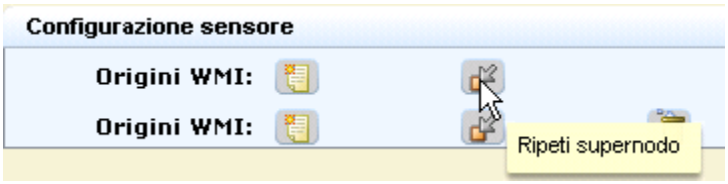
9. Configurare le impostazioni WMILogSensor per il computer locale per la raccolta di registri basata sugli agenti. Per ulteriori informazioni, fare clic sul link Aiuto.

   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 User Activity Reporting Module 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 User Activity Reporting Module.

Visualizzazione dei registri dalle origini evento di Windows

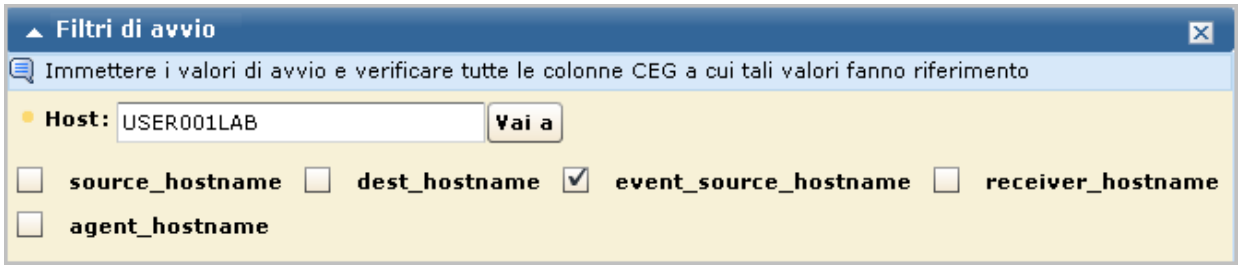
Uno dei modi più veloci per visualizzare i risultati delle query negli eventi in ingresso è utilizzare il Prompt dell'host. È anche possibile selezionare query o rapporti.

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.



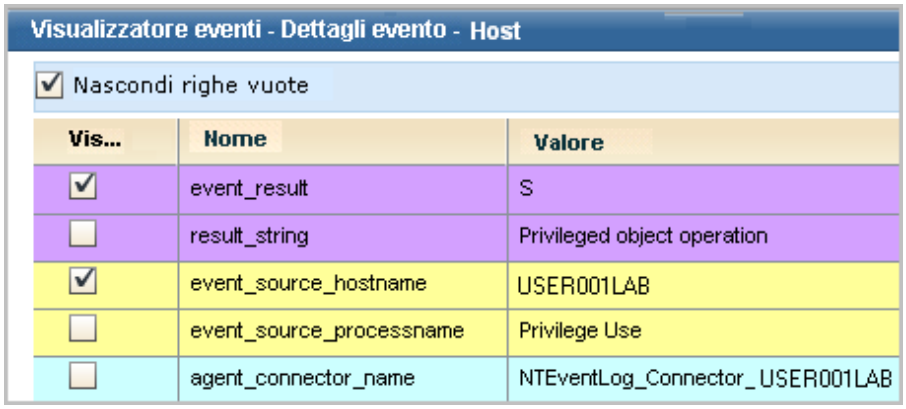
Vengono visualizzati gli eventi provenienti dalle origini evento del server WMI.

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:

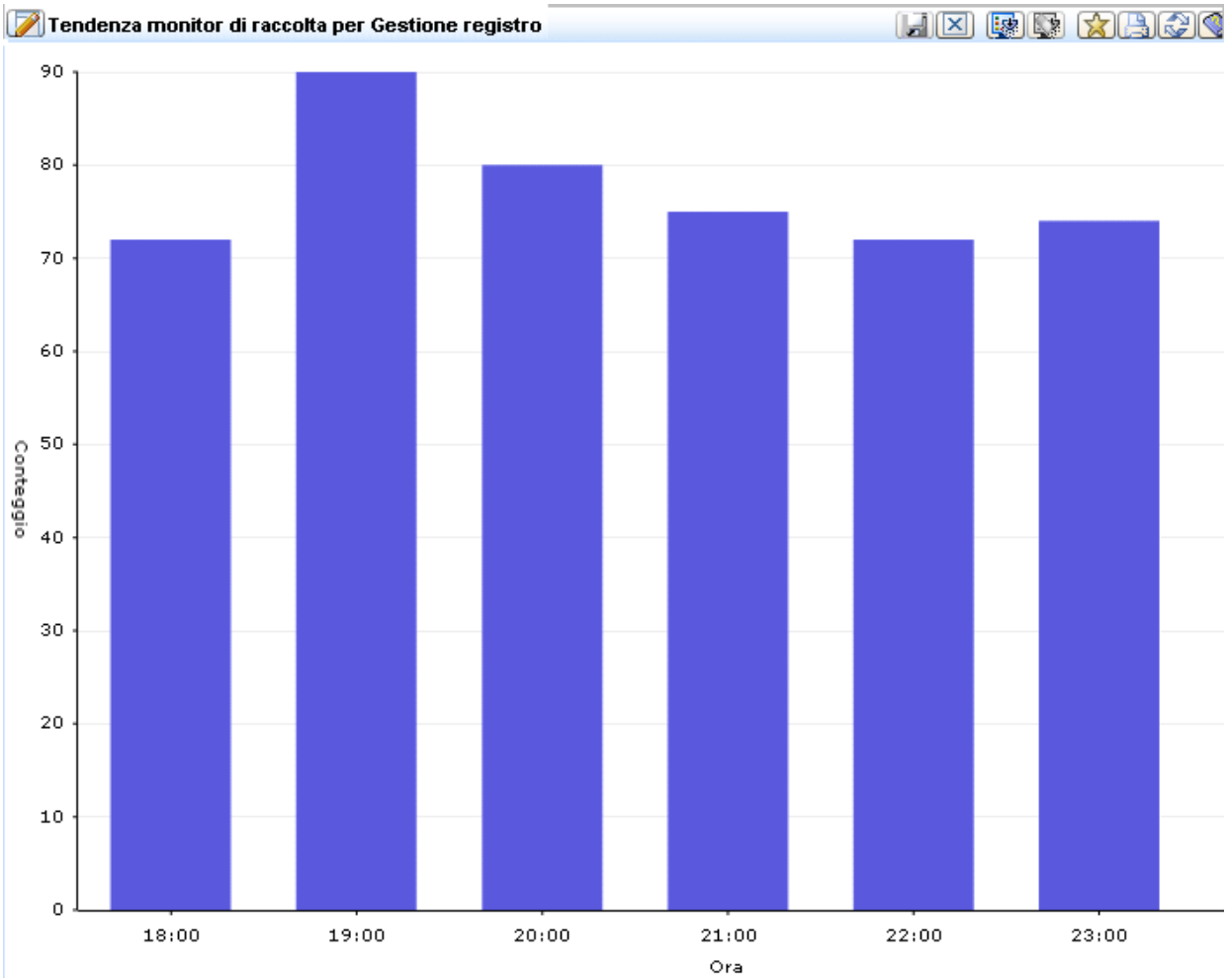
Livello di gravità CA	Utente di origine	Risultato	Categoria	Azione	Nome log
Avviso	calm_agent	S	System Access	Privilege Use	NT-Security

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:



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 User Activity Reporting Module.

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

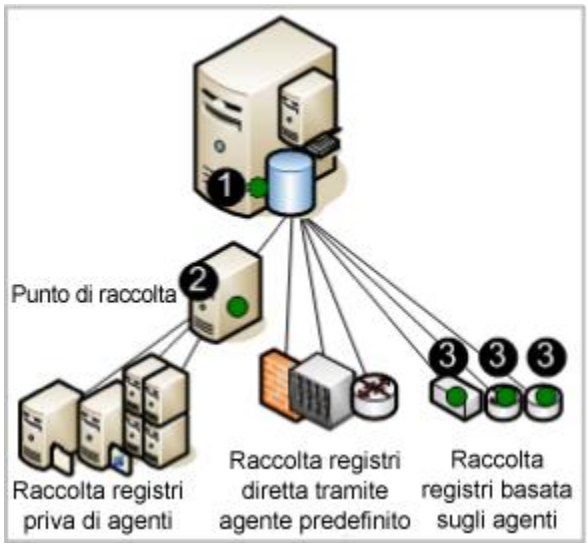
Capitolo 4: Funzionalità principali

Questa sezione contiene i seguenti argomenti:

Raccolta registri

Il server CA User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module.
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 User Activity Reporting Module 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 User Activity Reporting Module.

- 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

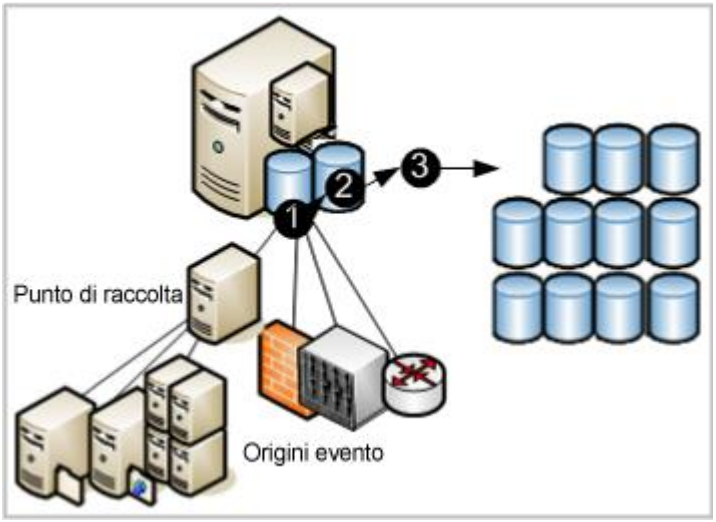
  Con la raccolta basata su agenti, viene installato un agente dove una o più origini di eventi sono in esecuzione ed è configurato un connettore per ogni origine di evento.

  Vantaggio: è possibile raccogliere i registri da un'origine dove la larghezza di banda della rete tra l'origine e CA User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module. 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 User Activity Reporting Module 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 User Activity Reporting Module* 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 User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module*.

Avviso di violazione del criterio

CA User Activity Reporting Module 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 User Activity Reporting Module 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

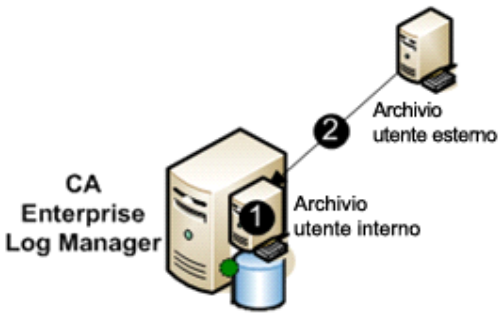
Gli elenchi con chiave possono essere aggiornati manualmente, importando un file o eseguendo una procedura CA IT PAM di valori dinamici.

Nota: per i dettagli sugli avvisi consultare la *Guida all'amministrazione di CA User Activity Reporting Module*.

Gestione delle adesioni

Al momento di configurare l'archivio utenti, si sceglie se utilizzare l'archivio utenti predefinito su CA User Activity Reporting Module 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 User Activity Reporting Module 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.

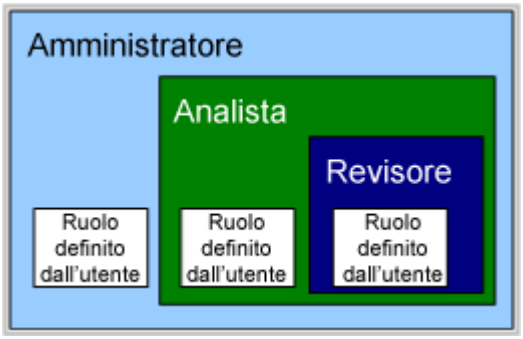
Nota: per informazioni sulla configurazione dell'accesso utente di base, consultare la *Guida all'implementazione CA User Activity Reporting Module*. Per informazioni sui criteri che supportano ruoli predefiniti, sulla creazione di account utente e sull'assegnazione di ruoli, consultare la *Guida all'amministrazione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

Accesso in base ai ruoli

CA User Activity Reporting Module 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 User Activity Reporting Module:

- 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 User Activity Reporting Module* 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 User Activity Reporting Module. 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 User Activity Reporting Module, 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 User Activity Reporting Module contatta il server di sottoscrizione CA per gli aggiornamenti e scarica tutti i nuovi aggiornamenti disponibili. Il server CA User Activity Reporting Module 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 User Activity Reporting Module.
2. Come client di sottoscrizione, il server CA User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module

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 User Activity Reporting Module nella visualizzazione corrente.

Per visualizzare tooltip e altri aiuti

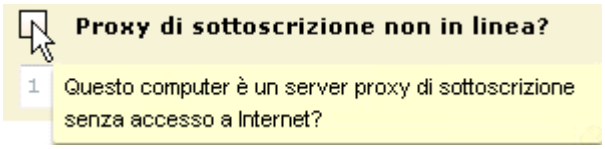
1. Spostare il cursore sui pulsanti per visualizzare la descrizione della relativa funzione. In questo modo è possibile visualizzare la funzione di tutti i pulsanti.

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

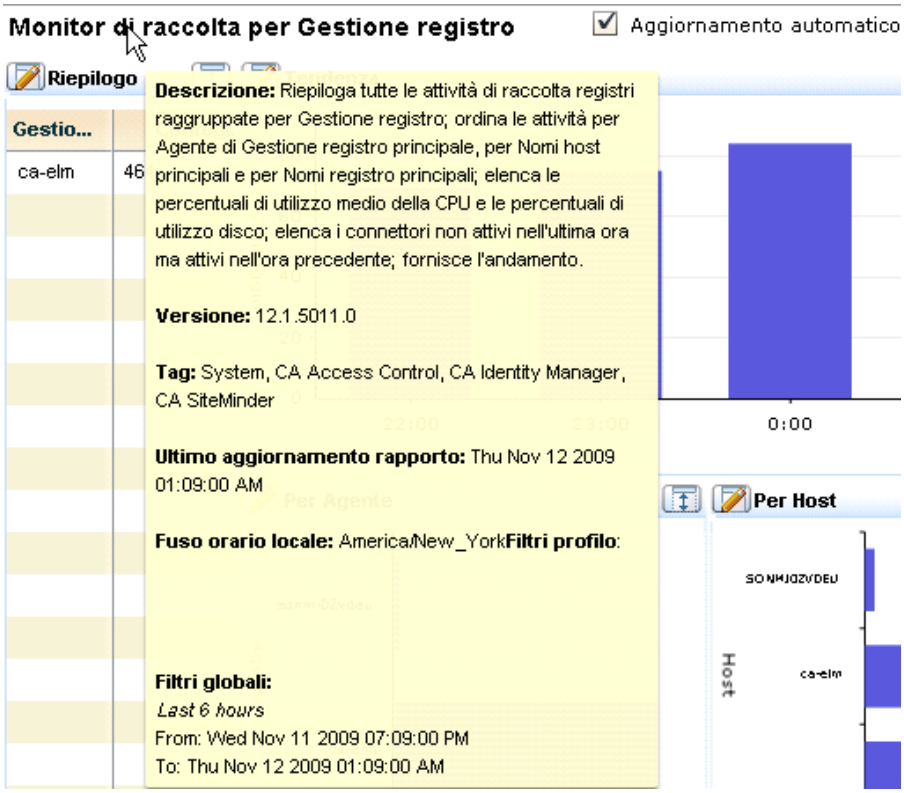
   I pulsanti attivi abilitati sono visualizzati a colori. Ad esempio, gli amministratori della gestione di utenti e accessi visualizzano il pulsante Elenco filtri di accesso a colori.

   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.

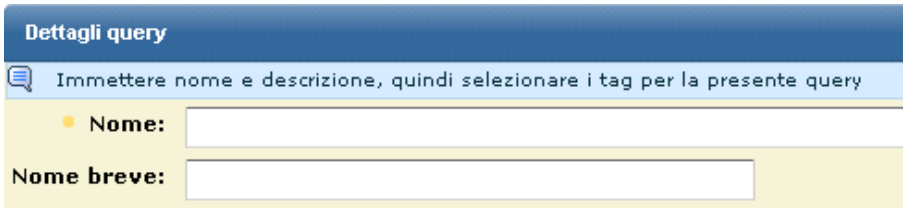
3. Visualizzare le descrizioni relative ai campi di inserimento o alle caselle di controllo spostando il cursore sul nome del campo.



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.

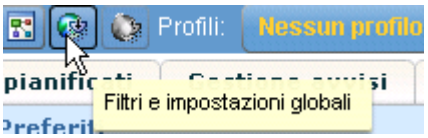
Per visualizzare la Guida in linea

1. Fare clic sul link Aiuto nella barra degli strumenti per visualizzare l'applicazione Guida in linea di CA User Activity Reporting Module.

Si aprirà la Guida in linea di CA User Activity Reporting Module, i cui contenuti vengono visualizzati nel riquadro a sinistra.

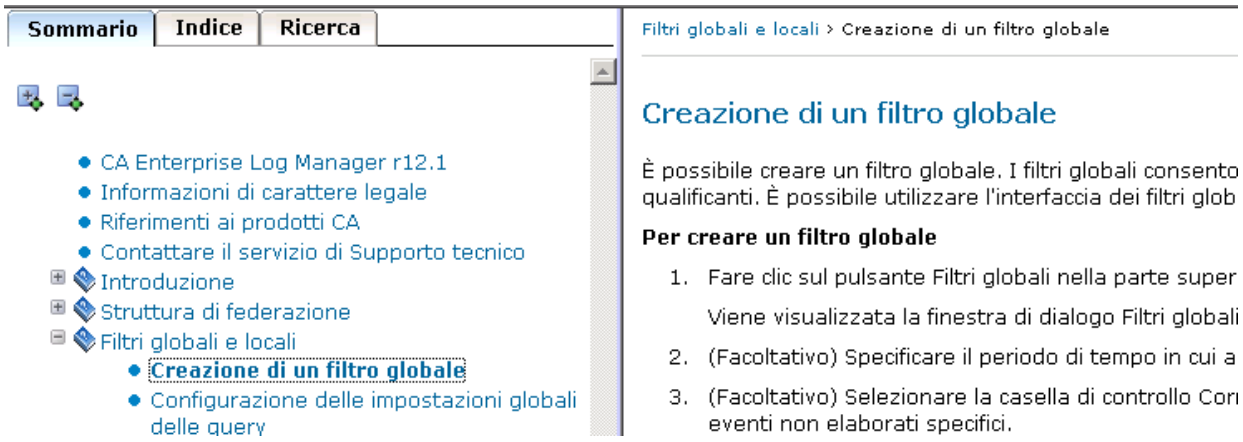
2. Accedere alla guida sensibile al contesto dal pulsante Aiuto come mostrato nell'esempio seguente.

   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 User Activity Reporting Module, 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.

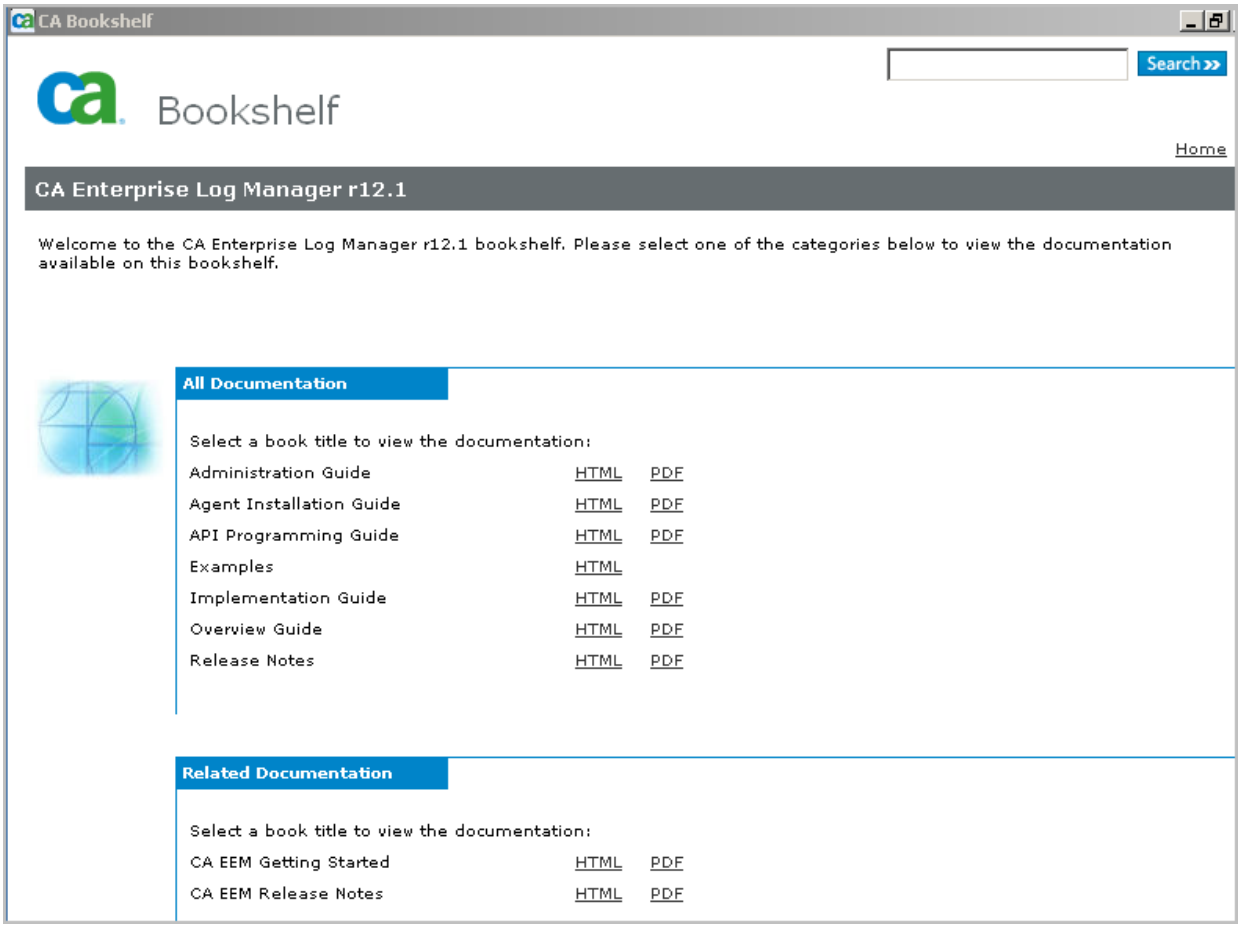
Esplorazione della Bookshelf della documentazione

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:

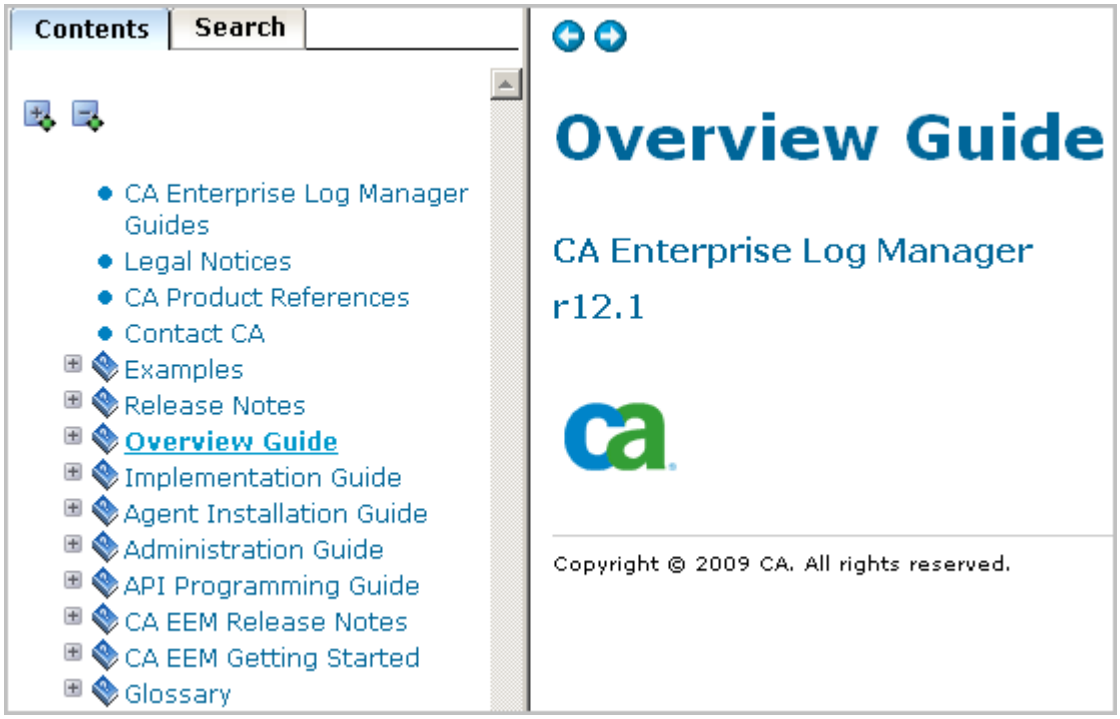


Seguono le descrizioni del contenuto delle guide principali accompagnate da esempi:

Documentazione	Descrive come
Guida all'installazione degli agenti	Installare agenti
Guida all'implementazione	Installare e configurare un sistema CA User Activity Reporting Module.
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.



Indice