AUTHORIZED DOCUMENTATION

Guida dell'utente

October 31, 2008

Novell®
Identity Audit

1.0

www.novell.com

Note legali

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
USA
www.novell.com

Documentazione online: per accedere alla documentazione online più recente relativa a questo e ad altri prodotti Novell, vedere la pagina Web relativa alla documentazione di Novell (http://www.novell.com/documentation).

Marchi di fabbrica di Novell

Per informazioni sui marchi di fabbrica di Novell, vedere l'elenco di marchi di fabbrica e di servizio di Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiali di terze parti

Tutti i marchi di fabbrica di terze parti appartengono ai rispettivi proprietari.

Sommario

Informazioni sulla Guida

Questa guida illustra l'installazione e la configurazione di Novell® Identity Audit.

Destinatari

Questa guida è destinata agli amministratori di Novell Identity Audit.

Feedback

È possibile inviare i propri commenti e suggerimenti relativi a questo manuale e agli altri documenti forniti con questo prodotto. Utilizzare la funzione Commenti degli utenti disponibile nella parte inferiore di ogni pagina della documentazione online oppure visitare il sito Web all'indirizzo www.novell.com/documentation/feedback.html per inviare commenti.

Aggiornamenti della documentazione

Per ottenere la versione più recente della *Guida dell'utente di Novell Identity Audit 1.0*, visitare il sito Web della documentazione di Identity Audit (http://www.novell.com/documentation/identityaudit).

Convenzioni della documentazione

Nella documentazione di Novell il simbolo maggiore di (>) viene utilizzato per separare le azioni di uno stesso passo di procedura e gli elementi in un percorso di riferimenti incrociati.

Un simbolo di marchio di fabbrica (®, ™ e così via) denota un marchio di fabbrica Novell. Un asterisco (*) denota un marchio di fabbrica di terze parti.

Introduzione

1

Novell® Identity Audit fornisce funzionalità di monitoraggio degli eventi e di generazione di rapporti a essi relativi per l'ambiente di gestione dell'identità e della sicurezza di Novell che include Novell eDirectory™, Novell Identity Manager, Novell Access Manager, Novell Modular Authentication Services (NMAS™), Novell SecureLogin, e Novell SecretStore®.

1.1 Panoramica sul prodotto

Novell Identity Audit 1.0 è un agile strumento di facile utilizzo per la raccolta, l'aggregazione e l'archiviazione di eventi generati da Novell Identity Manager, Novell Access Manager, Novell eDirectory e altri prodotti e tecnologie Novell associati all'identità e alla sicurezza. Le funzioni principali comprendono:

- Interfacce di amministrazione e generazione di rapporti basate su Web.
- Uno strumento di ricerca di tutti gli eventi che consente ricerche in più campi evento.
- Output di eventi selezionati verso numerosi canali.
- Il motore incorporato di Jasper Reports per consentire l'utilizzo di strumenti open source per la personalizzazione dei rapporti inclusi nel prodotto o per la creazione di nuovi rapporti.
- Il database incorporato elimina la necessità di amministrare un database esterno, nonché di acquisire le relative licenze.
- Strumenti per la gestione dei dati semplici e intuitivi

1.1.1 Confronto con Novell Audit 2.0.2

Novell Identity Audit 1.0 è progettato per sostituire la linea di prodotti Novell Audit, per la quale il supporto generico verrà interrotto nel febbraio 2009. Le funzioni di Identity Audit sono paragonabili a quelle di Novell Audit, ma sono stati apportati importanti miglioramenti all'architettura, alla generazione dei rapporti e alla gestione dei dati. Novell Identity Audit 1.0 è la sostituzione immediata relativa al server di registrazione sicuro di Novell Audit 2.0.2 per i prodotti della linea relativa all'identità e alla sicurezza di Novell. Poiché in Novell Identity Audit viene utilizzato un nuovo database incorporato, si consiglia di conservare gli eventi di Novell Audit esistenti nel database archiviato di quest'ultimo prodotto piuttosto che tentare una migrazione dei dati esistenti.

Il componente client di Novell Audit, denominato Platform Agent, è ancora utilizzato in Novell Identity Audit come meccanismo per il trasporto dei dati. Il componente continuerà a essere supportato, in conformità con quanto stabilito in relazione al ciclo di vita dei prodotti Novell per la gestione dell'identità e dell'accesso che ancora utilizzano Platform Agent.

1.1.2 Confronto con Novell Sentinel

Novell Identity Audit è sviluppato su solide fondamenta tecnologiche, in quanto condivide gran parte del codice soggiacente con Novell Sentinel. Tuttavia, Sentinel raccoglie i dati da una gamma più ampia di dispositivi, supporta una frequenza di eventi più alta e mette a disposizione più strumenti rispetto a Novell Identity Audit. Sentinel fornisce funzioni aggiuntive relative alle informazioni sulla sicurezza e alla gestione degli eventi (SIEM, Security Information and Event Management), quali dashboard in tempo reale, correlazione fra più eventi, controllo dei casi e riparazione automatica e raccolta di dati da prodotti non Novell. Identity Audit è progettato per essere integrato in future distribuzioni di Sentinel.

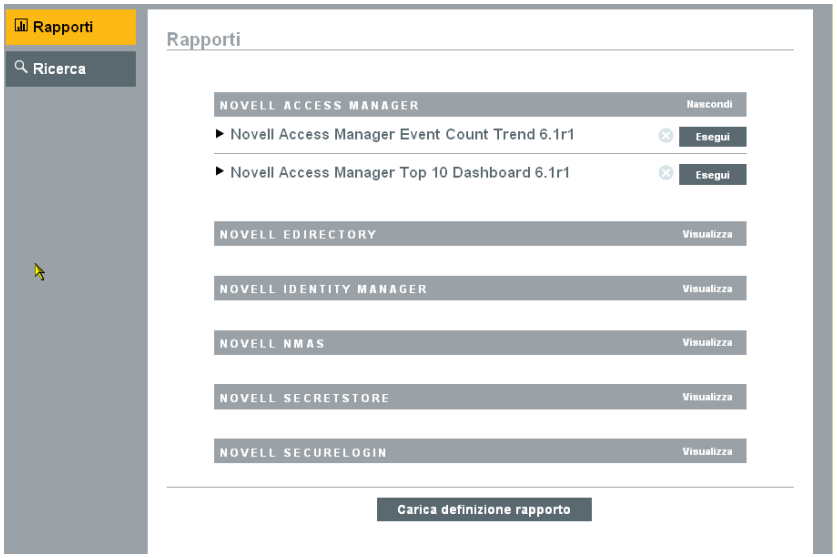
Novell Identity Audit non fa parte della piattaforma per la gestione della conformità (CMP, Compliance Management Platform) di Novell e non include le funzioni avanzate di integrazione di identità e sicurezza disponibili in questa piattaforma. Attualmente il componente relativo alla gestione della conformità per la revisione e il monitoraggio dell'identità è Sentinel 6.1.

1.2 Interfaccia

L'interfaccia Web di Novell Identity Audit consente di effettuare le seguenti attività:

- Caricamento, esecuzione, visualizzazione ed eliminazione di rapporti.
- Ricerca di eventi.
- Modifica dei dettagli dei profili utente.
- Creazione, modifica ed eliminazione di utenti, nonché assegnazione di diritti amministrativi (solo amministratori).
- Configurazione della raccolta di dati e visualizzazione dell'integrità delle origini degli eventi (solo amministratori).
- Configurazione dell'archiviazione dei dati e visualizzazione dell'integrità del database (solo amministratori).
- Creazione di regole di filtraggio e configurazione di azioni associate per inviare dati di eventi corrispondenti a canali di output (solo amministratori).

Figura 1-1 *Interfaccia di Novell Identity Audit (visualizzazione amministratori)*



L'interfaccia si aggiorna automaticamente ogni 30 secondi per mostrare gli aggiornamenti di altri utenti, se disponibili.

L'interfaccia è disponibile in più lingue, vale a dire inglese, francese, tedesco, italiano, giapponese, portoghese, spagnolo, cinese semplificato e cinese tradizionale. La lingua di default dell'interfaccia è quella di default del browser, ma è possibile selezionare un'altra lingua al momento del login.

Nota: anche se l'interfaccia è localizzata in lingue a doppio byte, la versione corrente di Identity Audit non consente l'elaborazione dei dati degli eventi a doppio byte.

1.3 Architettura

Identity Audit consente di raccogliere dati da più applicazioni relative all'identità e alla sicurezza di Novell. Questi server di applicazione sono configurati per generare record di eventi e ciascuno di essi ospita un agente di piattaforma, che fa parte dell'applicazione Novell Audit. I dati degli eventi vengono inoltrati da un agente di piattaforma a un connettore di Audit presente nel server di Identity Audit.

Il connettore di Audit passa gli eventi al componente di raccolta dei dati, che analizza gli eventi e li colloca nel bus di comunicazione, ossia il backbone del sistema, e funge da broker di tutte le comunicazioni tra i componenti. Come parte della raccolta dei dati, gli eventi in entrata vengono valutati in base a una serie di regole di filtraggio. Queste regole consentono di filtrare gli eventi e di inviarli ai canali di output come un file, un relay SysLog o un .

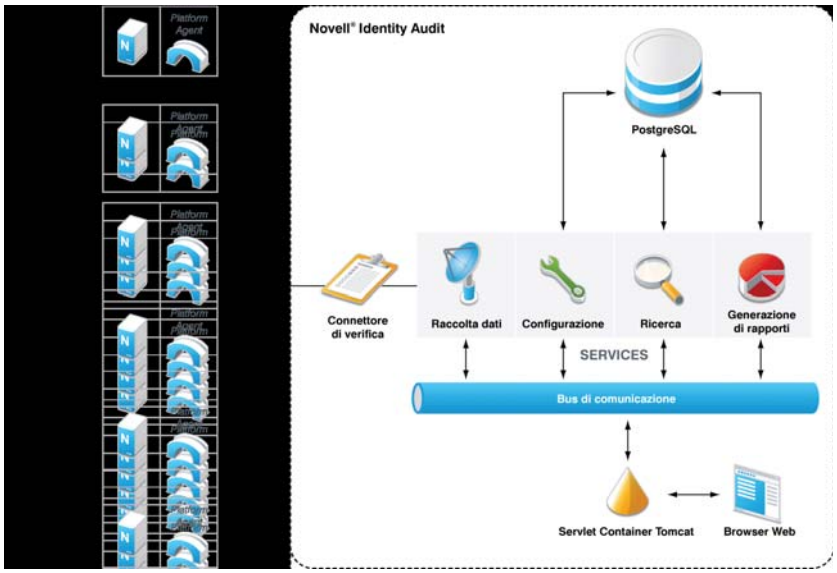
Tutti gli eventi, inoltre, vengono archiviati nel database di Identity Audit (di PostgreSQL*), in tabelle partizionate.

Il componente di configurazione consente di recuperare, aggiungere e modificare le informazioni di configurazione come la raccolta di dati e le impostazioni di archiviazione e le definizioni delle regole e dei rapporti. Consente inoltre di gestire l'autenticazione dell'utente.

Il componente di ricerca permette di eseguire rapide ricerche indicizzate e di recuperare gli eventi dal database per presentare i risultati della ricerca all'utente.

Il componente di generazione dei rapporti consente di eseguire i rapporti e di formattarne i risultati.

Figura 1-2 *Architettura di Identity Audit*



Gli utenti interagiscono con il server di Identity Audit e con tutte le funzionalità relative attraverso un browser Web, che si collega a un server Web Apache Tomcat. Il server Web effettua chiamate ai vari componenti di Identity Audit tramite il bus di comunicazione.

Requisiti di sistema

2

Oltre ai requisiti relativi all'hardware, al sistema operativo, al browser e alla compatibilità con le origini degli eventi elencati più avanti, per poter creare l'utente e il gruppo novell, che fungono da proprietari dei processi in esecuzione per Identity Audit, è necessario che l'installazione acceda al sistema operativo come utente root.

2.1 Requisiti hardware

Novell Identity Audit™ è supportato su hardware Xeon* e AMD Opteron* a 64 bit. Non è supportato su hardware Itanium. È consigliabile disporre dell'hardware riportato di seguito per un sistema di produzione in grado di contenere 90 giorni di dati online:

- 1 x Quad Core (x86-64)
- 16 GB di RAM
- 1,5 TB di spazio utilizzabile su disco - 3 unità (utilizzabili) da 500 GB e 10000 RPM in una configurazione hardware RAID
  - Circa 2/3 dello spazio su disco utilizzabile viene impiegato per i file del database.
  - Circa 1/3 dello spazio su disco utilizzabile viene impiegato per l'indice di ricerca e i file temp.
  - Una piccola quantità di spazio di archiviazione è disponibile per i dati archiviati che sono stati rimossi dal database, ma è consigliabile spostare i file dei dati archiviati in un altro supporto.

Tabella 2-1 *Prestazioni*

Unità di misura	Valore	Descrizione
Eventi per secondo (eps) - stato regolare	100	Frequenza media di eventi durante il normale funzionamento
Eventi per secondo (eps) - picco	500	Frequenza massima di eventi durante un sovraccarico (fino a 10 minuti)

Unità di misura	Valore	Descrizione
Eventi per secondo (eps) - picco per applicazione	300	Frequenza massima di eventi di ogni tipo di applicazione Novell ◆ Le percentuali di eventi sono in genere basse (meno di 15 eps) per Identity Manager, SecureLogin, SecretStore® e NMAS™. ◆ Le percentuali di eventi possono essere molto elevate in eDirectory™ e Access Manager. Il filtro degli eventi deve essere implementato per garantire una frequenza gestibile. ◆ Anche durante un sovraccarico di eventi, nessuna applicazione può inviare più del numero di eventi per secondo stabilito.
Dati online	90 giorni o 750 milioni di eventi	Quantità di dati che può essere archiviata da Identity Audit a una frequenza dello stato regolare di circa 100 eps, con lo spazio di archiviazione consigliato.

2.2 Sistemi operativi supportati

L'esecuzione di Identity Audit è garantita su SuSE Linux Enterprise Server™ 10 SP1 e SP2 a 64 bit.

2.3 Browser supportati

I browser elencati di seguito sono supportati da Identity Audit. Se si utilizzano altri browser, è possibile che i dati non vengano visualizzati nel modo previsto.

Tabella 2-2 *Browser Web supportati da Novell Identity Audit*

Browser Web e versione
Mozilla Firefox 2
Mozilla Firefox 3
Microsoft Internet Explorer 7

Le prestazioni delle ricerche e della visualizzazione dei rapporti sembrano variare in base al browser. Novell ha rilevato prestazioni particolarmente buone in Mozilla Firefox 3.

2.4 Platform Agent supportato

Identity Audit 1.0 supporta la raccolta di eventi per i log da molte applicazioni che sono supportate da Novell Audit e dal relativo agente di piattaforma. Per le origini degli eventi a 32 bit è necessario Platform Agent versione 2.0.2 FP6 (2.0.2.55) o successiva per Identity Audit. Per le origini degli eventi a 64 bit è necessario Platform Agent versione 2.0.2 FP6.

Nota: Alcune applicazioni Novell sono incluse in pacchetti con una versione precedente dell'agente di piattaforma. Nella versione consigliata sono incluse importanti correzioni di problemi. Pertanto si consiglia di aggiornare Platform Agent.

2.5 Origini degli eventi supportate

Identity Audit supporta la raccolta dei dati dalle applicazioni relative all'identità e alla sicurezza di Novell. Alcune applicazioni richiedono un livello di percorso specifico per raccogliere correttamente i dati.

Tabella 2-3 *Applicazioni supportate da Novell Identity Audit*

Applicazione
Novell Access Manager 3.0
Novell eDirectory 8.8.3 con la patch di strumentazione eDirectory disponibile nel sito Web di supporto di Novell (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~)
Novell Identity Manager 3.6
Novell NMAS 3.1
Novell SecretStore 3.4
Novell SecureLogin 6.0

Installazione

3

Questo capitolo illustra come installare Novell Identity Audit e come configurare le origini degli eventi per l'invio dei dati. Nelle istruzioni si dà per scontato che i requisiti minimi per ciascun componente del sistema siano stati soddisfatti. Per ulteriori informazioni, vedere il Capitolo 2, “Requisiti di sistema”, a pagina 13.

3.1 Installazione di Novell Identity Audit

Il pacchetto di installazione di Identity Audit consente di installare tutto il necessario per la sua esecuzione: l'applicazione e il bus dei messaggi di Identity Audit, il database in cui vengono archiviati gli eventi e i dati di configurazione, l'interfaccia utente basata sul Web e il server di generazione dei rapporti. Sono disponibili due opzioni di installazione: un'installazione semplice eseguibile come utente root o un'installazione a più fasi in cui l'utente root viene utilizzato il meno possibile.

3.1.1 Installazione rapida (come utente root)

Questa installazione semplice deve essere eseguita come utente root.

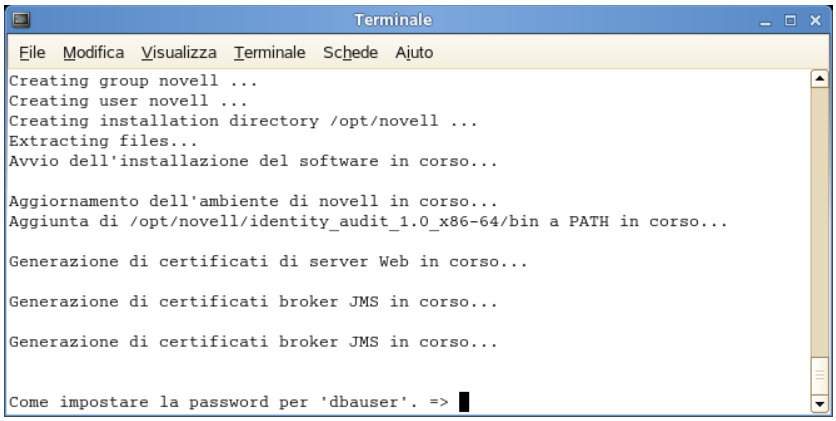
1. Eseguire il login come utente `root` al server in cui si desidera installare Identity Audit.
2. Scaricare o copiare `identity_audit_1.0_x86-64.tar.gz` in una directory temporanea.
3. Estrarre lo script di installazione dal file utilizzando il seguente comando:

   ```
   tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup/root_install_all.sh
   ```
4. Eseguire lo script `root_install_all.sh` utilizzando il seguente comando:

   ```
   identity_audit_1.0_x86-64/setup/root_install_all.sh identity_audit_1.0_x86-64.tar.gz
   ```
5. Selezionare una lingua immettendo un numero.

   Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.
6. Leggere il contratto di licenza con l'utente finale e immettere `1` o `y` se si accettano i termini e si desidera continuare l'installazione.

   L'installazione ha inizio. Se la lingua selezionata in precedenza non è disponibile per il programma di installazione, ad esempio il polacco, l'installazione continuerà in inglese.



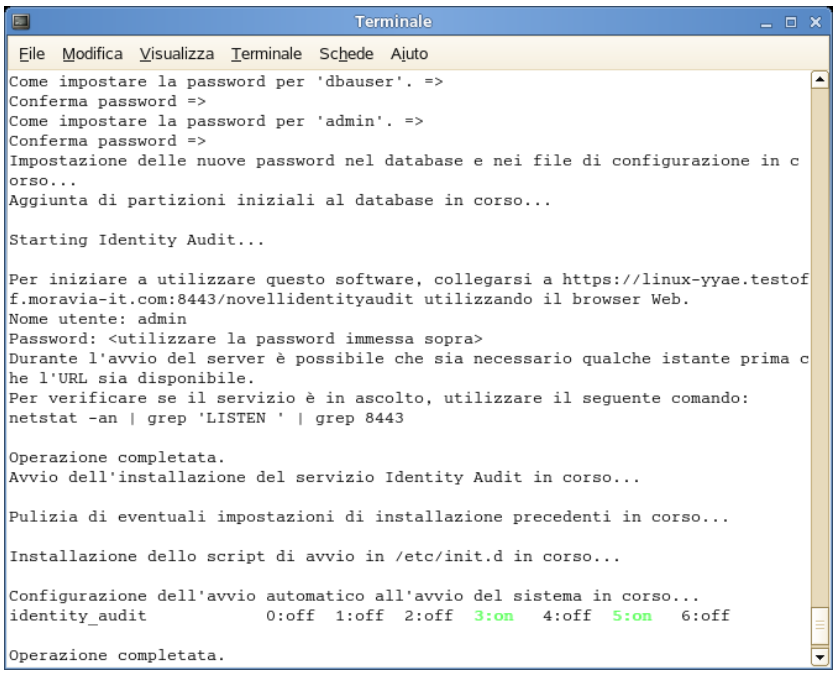
Se non sono già presenti, vengono creati l'utente e il gruppo novell.

7 Immettere la password per l'amministratore del database (dbauser).

8 Confermare la password per l'amministratore del database (dbauser).

9 Immettere la password dell'utente admin.

10 Confermare la password dell'utente admin.



Le credenziali di dbauser vengono utilizzate per creare le tabelle e le partizioni nel database PostgreSQL. Identity Audit è configurato per l'avvio con livelli di runtime 3 e 5 (in modalità multi utente con l'avvio in console o in modalità X-Windows).

Dopo l'avvio del servizio Identity Audit, è possibile eseguire il login all'URL specificato nell'output dell'installazione (https://hostIP:8443/novellidentityaudit). L'elaborazione degli eventi di revisione interni viene avviata immediatamente e la funzionalità del sistema sarà completa quando le origini degli eventi saranno state configurate per l'invio di dati a Identity Audit.

3.1.2 Installazione per utente non root

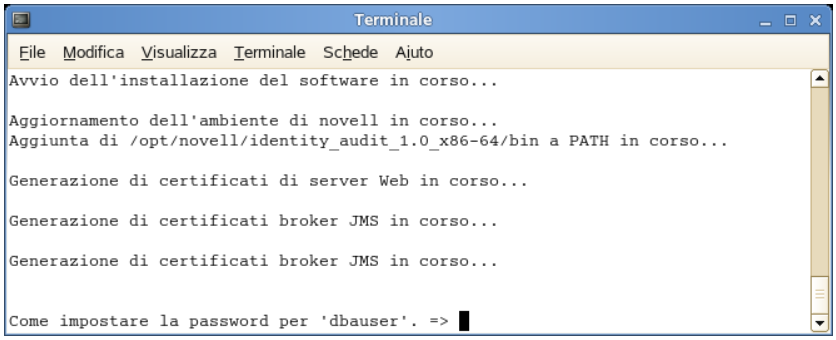
Se le norme dell'organizzazione non consentono l'esecuzione dell'intero processo di installazione come utente `root`, è possibile eseguire l'installazione in due fasi. La prima parte dell'installazione deve essere eseguita utilizzando l'accesso a livello root, mentre la seconda parte viene eseguita come utente amministrativo di Identity Audit, che viene creato durante la prima fase.

1. Eseguire il login come utente `root` al server in cui si desidera installare Identity Audit.
2. Scaricare o copiare `identity_audit_1.0_x86-64.tar.gz` nella directory `/tmp`.
3. Se l'utente e il gruppo novell non sono già presenti nel server:
   1. Estrarre lo script necessario per la creazione del gruppo e dell'utente novell dal file tar di Identity Audit. Ad esempio:
      ```
      tar xfz identity_audit_1.0_x86-64.tar.gz
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
   2. Eseguire lo script come utente `root` utilizzando il seguente comando:
      ```
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
      Il gruppo e l'utente novell saranno i proprietari dell'installazione e dei processi di Identity Audit.
4. Creare una directory per Identity Audit. Ad esempio:

   mkdir -p /opt/*novell*
5. Impostare l'utente e il gruppo novell come proprietari della directory. Ad esempio:
   ```
   chown -R novell:novell /opt/novell
   ```
6. Eseguire il login come utente novell:
   ```
   su novell
   ```
7. Estrarre il contenuto del file tar di Identity Audit nella directory appena creata. Ad esempio:
   ```
   cd /opt/novell
   tar xfz /tmp/identity_audit_1.0_x86-64.tar.gz
   ```
8. Eseguire lo script di installazione. Ad esempio:
   ```
   /opt/novell/identity_audit_1.0_x86-64/setup/install.sh
   ```
9. Selezionare una lingua immettendo un numero.

   Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.
10. Leggere il contratto di licenza e immettere `1` o `y` se si accettano i termini e se si desidera continuare l'installazione.

    L'installazione ha inizio. Se la lingua selezionata in precedenza non è disponibile per il programma di installazione, ad esempio il polacco, l'installazione continuerà in inglese.



11 Immettere la password per l'amministratore del database (dbauser).

12 Confermare la password per l'amministratore del database (dbauser).

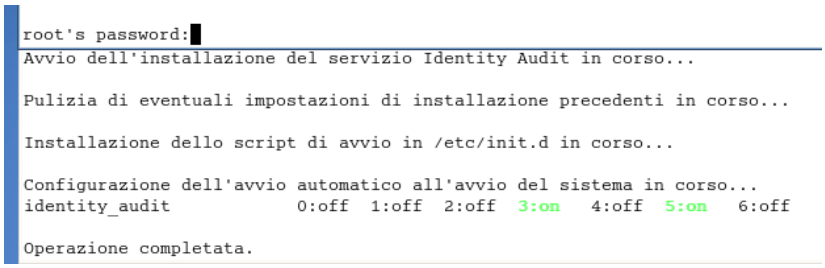
13 Immettere la password dell'utente admin.

14 Confermare la password dell'utente admin.

15 Eseguire il logout, quindi rieseguire il login come novell. Mediante questa operazione si otterrà il caricamento delle modifiche alla variabile di ambiente PATH apportate dallo script `install.sh`.

16 Eseguire lo script `root_install_service.sh` per abilitare l'avvio di Identity Audit come servizio. Questo passaggio richiede l'accesso a livello `root`. Ad esempio:

```
sudo /opt/novell/identity_audit_1.0_x86-64/setup/
root_install_service.sh
```



17 Immettere la password dell'utente `root`.

Identity Audit è configurato per l'avvio con livelli di runtime 3 e 5 (in modalità multi utente con l'avvio in console o in modalità X-Windows).

Dopo l'avvio del servizio Identity Audit, è possibile eseguire il login all'URL specificato nell'output dell'installazione (https://hostIP:8443/novellidentityaudit). L'elaborazione degli eventi di revisione interni viene avviata immediatamente e la funzionalità del sistema sarà completa quando le origini degli eventi saranno state configurate per l'invio di dati a Identity Audit.

3.2 Configurazione delle origini degli eventi

Identity Audit 1.0 supporta la raccolta di eventi per i log dalle applicazioni già supportate dal prodotto Novell Audit precedente e Platform Agent. Prima di completare la procedura di questa sezione, assicurarsi che siano supportati i prodotti Novell. Per ulteriori informazioni, vedere la Sezione 2.4, “Platform Agent supportato”, a pagina 14.

3.2.1 Installazione di Platform Agent

Platform Agent deve essere almeno disponibile nella versione minima consigliata per Identity Audit. Per ulteriori informazioni, vedere la Sezione 2.4, “Platform Agent supportato”, a pagina 14. La versione di Platform Agent appropriata, a 32 o a 64 bit, deve essere installata o aggiornata in tutti i computer relativi alle origini degli eventi. Platform Agent è incluso nel download di Novell Audit dal sito Web di download di Novell (http://download.novell.com).

Per installare o aggiornare Platform Agent a 32 bit:

1. Scaricare il file `.iso` per Audit 2.0.2 FP6 o versione successiva nella directory /tmp nel computer delle origini degli eventi.
2. Creare una directory per Audit. Ad esempio, `mkdir -p audit202fp6`
3. Eseguire il login come utente `root`.
4. Montare il file Audit`.iso`.

   ```
   mount -o loop ./NAudit202.iso ./audit202fp6
   ```
5. Individuare la directory `audit202fp6`.
6. Individuare la directory appropriata per il sistema operativo nell'origine degli eventi. Ad esempio:

   ```
   cd Linux
   ```
7. Eseguire `pinstall.lin`.

   ```
   ./pinstall.lin
   ```
8. Leggere il contratto di licenza e immettere `y` se di desidera accettare i termini.
9. Immettere `P` per installare Platform Agent.
10. Immettere `Y` per conservare qualsiasi configurazione precedente del file `logevent.conf`.

    Platform Agent viene installato.
11. Per verificare che la versione di Platform Agent sia corretta, immettere il comando seguente:

    ```
    rpm -qa | grep AUDT
    ```

    La versione di novell-AUDTplatformagent deve essere almeno quella supportata elencata nella Sezione 2.4, “Platform Agent supportato”, a pagina 14.

Per installare o aggiornare Platform Agent a 64 bit, scaricare NAudit 2.0.2 FP6 e seguire le istruzioni incluse nella patch.

3.2.2 Configurazione di Platform Agent

Dopo l'installazione, la configurazione di Platform Agent deve comportare l'invio dei dati al server di Identity Audit e, se si desidera, l'invio delle firme degli eventi dalle origini degli eventi.

Avviso: La configurazione di Platform Agent per generare le firme può influire in modo negativo sulle prestazioni dei computer delle origini degli eventi.

Per configurare Platform Agent:

1. Effettuare il login nel computer delle origini degli eventi.
2. Aprire il file `logevent` per la modifica. Il file si trova in un percorso diverso in base al sistema operativo:
   - Linux: `/etc/logevent.conf`
   - Windows: `C:\WINDOWS\logevent.cfg`
   - NetWare: `SYS:\etc\logevent.cfg`
   - Solaris: `/etc/logevent.conf`
3. Impostare LogHost sull'indirizzo IP del server di Identity Audit.

4 Impostare LogEnginePort=1289. (Aggiungere questa voce se non è già presente.)

5 Se si desidera che l'origine degli eventi invii le firme degli eventi, immettere LogSigned=always.

6 Salvare il file.

7 Riavviare Platform Agent. Il metodo varia in base al sistema operativo e all'applicazione. Riavviare il computer o fare riferimento alla documentazione specifica dell'applicazione nel sito Web della documentazione di Novell (http://www.novell.com/documentation) per ulteriori istruzioni.

3.2.3 Configurazione del livello di revisione

Gli eventi per cui ciascuna applicazione genera i record sono configurati in modo diverso per ogni applicazione controllata da Identity Audit. Gli URL riportati di seguito contengono ulteriori informazioni su ciascuna applicazione.

- Access Manager (http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b8cvd2l.html#b8cvd2l)
- eDirectory (http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/b296n3h.html)
- Identity Manager (http://www.novell.com/documentation/idm36/idm_sentinel/data/bookinfo.html)
- NMAS (http://www.novell.com/documentation/nmas32/admin/index.html?page=/documentation/nmas32/admin/data/ahefojr.html)
- SecretStore (http://www.novell.com/documentation/secretstore33/index.html?page=/documentation/secretstore33/nssadm/data/bsqdjxv.htm)
- SecureLogin (http://www.novell.com/documentation/securelogin60/index.html (see the Auditing link))

3.3 Operazioni preliminari

L'utente amministrativo creato durante l'installazione può effettuare il login all'applicazione Identity Audit e creare altri utenti, eseguire rapporti precaricati, caricare nuovi rapporti, eseguire ricerche di eventi e altro ancora.

Per eseguire il login a Identity Audit:

1 Aprire un browser Web supportato. Per ulteriori informazioni, vedere la Sezione 2.3, “Browser supportati”, a pagina 14.

2 Aprire la pagina di login di Identity Audit (https://hostIP:8443/novellidentityaudit).

3 Se è il primo login a Identity Audit, verrà visualizzato un certificato. È necessario accettarlo per continuare.

4 Immettere `admin`.

5 Immettere la password configurata per l'utente admin durante l'installazione.

6 Selezionare la lingua in cui si desidera visualizzare l'interfaccia di Identity Audit (inglese, portoghese, francese, italiano, tedesco, spagnolo, giapponese, cinese tradizionale o cinese semplificato).

7 Fare clic su *Login*.

3.4 Disinstallazione

Per eseguire la pulizia completa di un'installazione di Identity Audit, è necessario eseguire lo script di disinstallazione, nonché alcuni passaggi manuali.

1 Effettuare il login al server di Identity Audit come utente `root`.

2 Arrestare il servizio Identity Audit:

```
/etc/init.d/identity_audit stop
```

3 Eseguire lo script di disinstallazione:

```
/opt/novell/identity_audit_1.0_x86-64/setup/
root_uninstall_service.sh
```

4 Eliminare la home directory di Identity Audit con il relativo contenuto.

```
rm -rf /opt/novell/identity_audit_1.0_x86-64
```

5 La procedura finale dipende dal fatto che si desideri conservare informazioni correlate al gruppo e all'utente novell.

- Se non si desidera conservare le informazioni correlate all'utente novell, eseguire il comando riportato di seguito per rimuovere l'utente, la home directory e il gruppo:

  ```
  userdel -r novell && groupdel novell
  ```

- Se non si desidera conservare l'utente novell e la relativa home directory, ma si desidera rimuovere tutte le impostazioni correlate a Identity Audit, attenersi alla seguente procedura:

  1. Rimuovere le voci delle variabili di ambiente riportate di seguito associate a Identity Audit dal profilo dell'utente novell (in `~novell/.bashrc`):

     ```
     APP_HOME=/opt/novell/identity_audit_1.0_x86-64 export
     PATH=$APP_HOME/bin:$PATH
     ```

  2. Rimuovere la voce dbauser dal file di PostgreSQL `~novell/.pgpass`.
     `*:*:*:dbauser:`*`password`*

     Nota: anche se la password di dbauser viene visualizzata in testo non cifrato, il contenuto di questo file è visibile solo per gli utenti novell e root, che hanno già l'accesso completo a tutte le funzioni del server di Identity Audit.

Esecuzione di ricerche

4

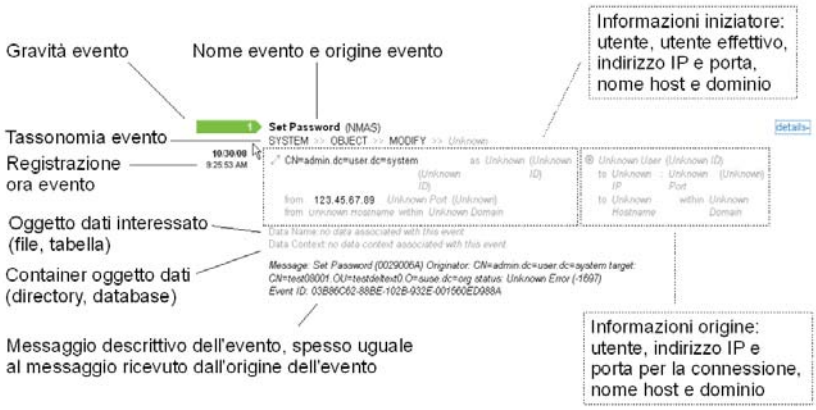
Questa sezione descrive le funzionalità di ricerca di Novell® Identity Audit.

4.1 Panoramica della ricerca di eventi

Novell Identity Audit consente di eseguire ricerche di eventi. Nella ricerca sono inclusi tutti i dati online attualmente presenti nel database. Tuttavia gli eventi interni generati dal sistema di Identity Audit vengono esclusi, a meno che l'opzione *Includi eventi di sistema* non sia selezionata. Per default, gli eventi vengono ordinati in base all'algoritmo di rilevanza del motore di ricerca.

Le informazioni di base sugli eventi comprendono il nome, l'origine, l'ora e la gravità dell'evento, informazioni sull'iniziatore (rappresentate da un'icona che raffigura una freccia) e informazioni sulla destinazione (rappresentate da un'icona che raffigura il centro di un bersaglio).

Figura 4-1 *Campi degli eventi*



4.2 Esecuzione di una ricerca di eventi

È possibile eseguire ricerche semplici e avanzate.

4.2.1 Ricerca semplice

Una ricerca semplice viene eseguita su tutti i campi degli eventi elencati nella Tabella 4-1 a pagina 30. Alcuni esempi di ricerca semplice comprendono quanto riportato di seguito:

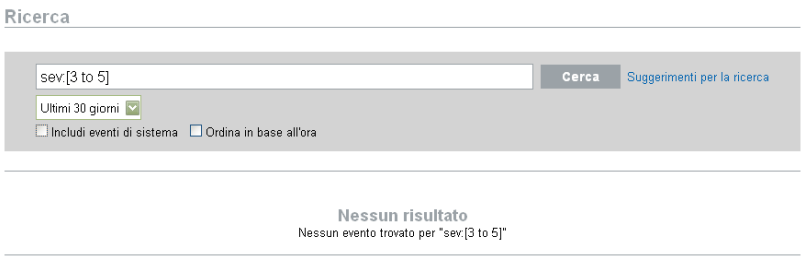
- `root`
- `127.0.0.1`
- `Blocco*`
- `driverset0`

Nota: se l'ora non è sincronizzata tra il computer dell'utente finale e il server di Identity Audit (ad esempio nel caso in cui un computer è in ritardo di 25 minuti), si potrebbero ottenere risultati imprevisti dalla ricerca. Le ricerche come *Last 1 hour* o *Last 24 hours* si basano sull'ora del computer dell'utente finale.

---

1. Fare clic sul collegamento *Ricerca* a sinistra.

   Identity Audit viene configurato per l'esecuzione di una ricerca di default di eventi non di sistema con gravità da 3 a 5 la prima volta che si fa clic sul collegamento *Ricerca*. In caso contrario verrà impostata la ricerca di default dell'ultimo termine immesso dall'utente.



2. Per una ricerca diversa, digitare un termine di ricerca nel campo apposito (ad esempio `admin`). Nella ricerca le differenze fra maiuscole e minuscole non vengono rilevate.
3. Selezionare il periodo di tempo per il quale eseguire la ricerca. Il significato della maggior parte delle opzioni relative al periodo di tempo è esplicito. L'impostazione di default è *Ultimi 30 giorni*.
   - Se si seleziona *Personalizzato* è possibile selezionare la data e l'ora di inizio e di fine per l'interrogazione. La data di inizio deve essere precedente alla data di fine e l'ora si basa
   - Se si seleziona *Sempre*, la ricerca di tutti i dati viene eseguita nel database.
4. Selezionare *Includi eventi di sistema* per includere gli eventi generati durante l'esecuzione di operazioni del sistema di Identity Audit.
5. Selezionare *Sort By Time* per disporre i dati con gli eventi più recenti all'inizio.

   Nota: L'ordine in base all'ora richiede più tempo rispetto all'ordine in base all'importanza, che è il valore di default.

   ---

6. Fare clic su *Ricerca*.

   Il testo specificato viene ricercato in tutti i campi dell'indice. L'icona che raffigura una ruota che gira indica che la ricerca è in corso.

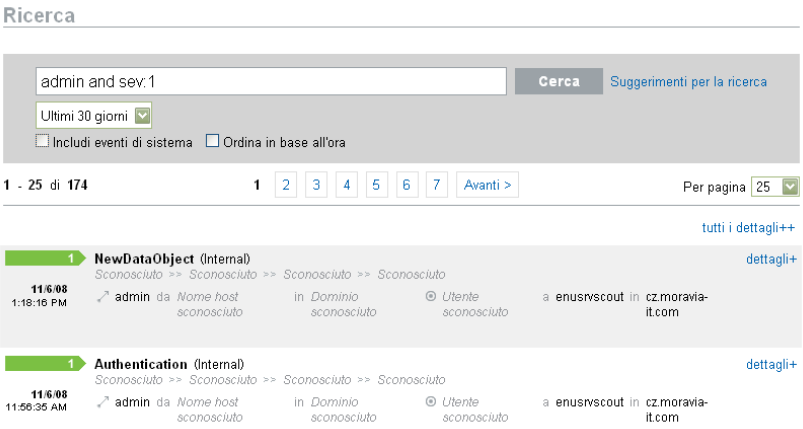
Al termine della ricerca vengono visualizzati i riepiloghi degli eventi.

4.2.2 Ricerca avanzata

La ricerca avanzata consente di cercare un valore in uno o più campi evento specifici. I criteri di ricerca avanzati sono basati sui nomi brevi di ciascun campo evento e sulla logica di ricerca per l'indice. Nella tabella riportata di seguito sono descritti i campi, vengono forniti i nomi brevi per le ricerche avanzate e si indica se i campi sono presenti nelle visualizzazioni degli eventi semplice e dettagliata.

Per cercare un valore in un campo specifico, utilizzare il nome breve del campo (per ulteriori informazioni, vedere la Tabella 4-1 a pagina 30), due punti e il valore. Ad esempio, per cercare un tentativo di autenticazione in Identity Audit da parte di user2, digitare il testo riportato di seguito nel campo della ricerca:

- `evt:authentication AND sun:user2`
- `pn:NMAS AND sev:5`
- `sip:123.45.67.89 AND evt:"Set Password"`



È possibile combinare più criteri di ricerca avanzati utilizzando i seguenti operatori booleani:

- AND (è necessario utilizzare le maiuscole)
- OR (è necessario utilizzare le maiuscole)
- NOT (è necessario utilizzare le maiuscole; l'operatore non può essere utilizzato come unico criterio di ricerca)
- +
- -

Per i caratteri speciali è necessario utilizzare sequenze di escape precedute dal simbolo \:

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
```

I criteri di ricerca avanzati sono modellati sui criteri di ricerca per il pacchetto open source Apache Lucene. Per ulteriori informazioni sui criteri di ricerca, visitare la pagina Web Lucene Query Parser Syntax (http://lucene.apache.org/java/2_3_2/queryparsersyntax.html).

4.3 Visualizzazione dei risultati della ricerca

Le ricerche restituiscono insiemi di eventi. È possibile visualizzare informazioni semplici o dettagliate sugli eventi e configurare il numero di risultati visualizzato per pagina. I risultati di ricerca vengono restituiti in gruppi. La dimensione di default dei gruppi è 25, ma è semplice impostare una dimensione diversa.

- Sezione 4.3.1, “Visualizzazione semplice degli eventi”, a pagina 28
- Sezione 4.3.2, “Visualizzazione dettagliata degli eventi”, a pagina 29
- Sezione 4.3.3, “Limitazione dei risultati di ricerca”, a pagina 29

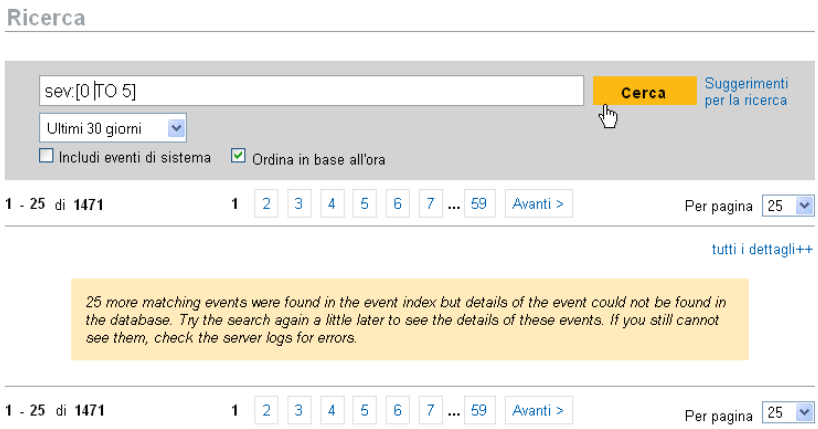
4.3.1 Visualizzazione semplice degli eventi

Le informazioni relative a ciascun evento sono raggruppate in informazioni sull'iniziatore e informazioni sulla destinazione. Se per un determinato campo evento non sono disponibili dati, questo viene etichettato come *Sconosciuto*.

Figura 4-2 *Visualizzazione semplice degli eventi*

Talvolta il motore di ricerca potrebbe indicizzare gli eventi più rapidamente di quanto vengano inseriti nel database. Se viene eseguita una ricerca che restituisce eventi che non sono stati inseriti nel database, viene visualizzato un messaggio che indica che alcuni eventi corrispondono all'interrogazione di ricerca, ma che non sono disponibili nel database. In genere se la ricerca viene eseguita di nuovo in un secondo tempo, gli eventi si troveranno nel database e la ricerca avrà esito positivo.

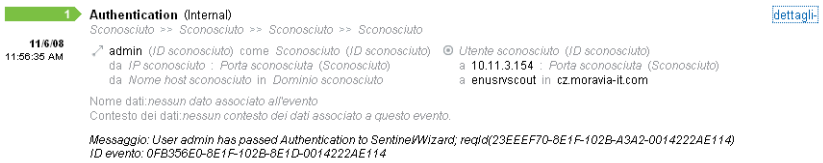
Figura 4-3 *Eventi indicizzati, ma non ancora nel database*



4.3.2 Visualizzazione dettagliata degli eventi

È possibile visualizzare dettagli aggiuntivi per uno o più eventi facendo clic sul collegamento *dettagli* nella parte destra della pagina. È possibile visualizzare o nascondere i dettagli di tutti gli eventi presenti in una pagina utilizzando il collegamento tutti i dettagli++ o *tutti i dettagli--*. L'opzione selezionata viene conservata durante la visualizzazione di più pagine di risultati oppure se si eseguono nuove ricerche.

Figura 4-4 *Visualizzazione dettagliata degli eventi*



L'evento precedente mostra lo stesso evento della Figura 4-2 a pagina 28, ma con una visualizzazione ampliata che presenta ulteriori campi di dati che potrebbero essere stati popolati.

4.3.3 Limitazione dei risultati di ricerca

Dopo aver visualizzato i risultati di una ricerca potrebbe essere necessario limitarli aggiungendo ulteriori criteri. Ad esempio, se il nome utente di un iniziatore compare molte volte nei risultati della ricerca, è possibile visualizzare altri eventi provenienti da quell'iniziatore.

Per filtrare i risultati della ricerca mediante un valore specifico presente nei risultati stessi:

1. Identificare i criteri desiderati per il filtro nei risultati della ricerca.
2. Fare clic sul valore (ad esempio target hostname test1900) con cui filtrare i risultati.

Suggerimento: in questo modo il valore viene aggiunto al filtro con un operatore AND. Per aggiungere il valore al filtro con un operatore NOT, premere Alt mentre si fa clic sul valore.

3. Fare clic su *Ricerca*.

Alcuni campi non possono essere selezionati per limitare una ricerca come descritto:

- EventTime
- Message
- Tutti i campi correlati al Reporter
- Tutti i campi correlati all'Observer
- Tutti i campi con il valore `Sconosciuto`

4.4 Campi degli eventi

Ogni evento dispone di campi che potrebbero essere o meno popolati, in base all'evento specifico. I valori per questi campi evento possono essere visualizzati mediante una ricerca o l'esecuzione di un rapporto. Ogni campo ha un nome breve utilizzato nelle ricerche avanzate. I valori per la maggior parte di questi campi sono disponibili nella visualizzazione dettagliata degli eventi. Altri valori sono anche presenti nella visualizzazione semplice degli eventi.

Tabella 4-1 *Campi degli eventi*

Campo	Nome breve	Descrizione	Presente in visualizzazione semplice	Presente in visualizzazione dettagliata
Severity	sev	Gravità dell'evento su una scala da 0 (informativo) a 5 (critico).	X	X
EventTime	dt	Registrazione dell'orario dell'evento. L'orario può corrispondere a quello del server di Identity Audit, oppure a quello registrato dall'origine dell'evento (se è abilitata l'opzione Considera affidabile l'ora dell'evento).	X	X
EventName	evt	Nome breve dell'evento.	X	X
Message	msg	Messaggio dettagliato associato all'evento.		X
ProductName	pn	Prodotto che ha generato l'evento, ossia l'origine dell'evento. Viene visualizzato dopo il nome dell'evento.	X	X

Campo	Nome breve	Descrizione	Presente in visualizzazione semplice	Presente in visualizzazione dettagliata
InitUserName	sun	Nome dell'utente responsabile dell'inizializzazione dell'evento.	X	X
InitUserID	iuid	ID dell'utente responsabile dell'inizializzazione dell'evento.		X
InitUserDomain	rv35	Dominio dell'utente responsabile dell'inizializzazione dell'evento. Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
InitHostName	shn	Nome host del computer a partire dal quale l'evento è stato inizializzato.	X	X
InitHostDomain	rv42	Dominio del computer a partire dal quale l'evento è stato inizializzato.	X	X
InitIP	sip	Indirizzo IP del computer a partire dal quale l'evento è stato inizializzato.		X
InitServicePort	spint	Numero della porta a partire dalla quale l'evento è stato inizializzato (ad esempio HTTP).		X
InitServicePortName	sp	Tipo della porta a partire dalla quale l'evento è stato inizializzato (ad esempio HTTP).		X
TargetUserName	dun	Nome dell'utente di destinazione dell'evento.	X	X
TargetUserID	tuid	ID dell'utente di destinazione dell'evento.		X
TargetUserDomain	rv35	Dominio dell'utente di destinazione dell'evento. Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		X
TargetHostName	dhn	Nome host del computer di destinazione dell'evento.	X	X
TargetHostDomain	rv45	Dominio del computer di destinazione dell'evento.	X	X
TargetIP	dip	Indirizzo IP del computer di destinazione dell'evento.		X
TargetServicePort	dpint	Numero della porta di destinazione dell'evento (ad esempio 80).		X
TargetServicePortName	dp	Tipo della porta di destinazione dell'evento (ad esempio HTTP).		X

Campo	Nome breve	Descrizione	Presente in visualizzazione semplice	Presente in visualizzazione dettagliata
TargetTrustName	ttn	Ruolo dell'utente di destinazione dell'evento (ad esempio FinanceAdmin) Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
TargetTrustID	ttid	ID numerico che rappresenta il ruolo dell'utente di destinazione dell'evento. Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
TargetTrustDomain	ttd	Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
EffectiveUserName	euname	Nome dell'utente impersonato da InitUser (ad esempio utente `root` che utilizza `su`). Nella visualizzazione dettagliata degli eventi, segue *Nome utente iniziatore (ID utente iniziatore*).		X
EffectiveUserID	euid	ID numerico dell'utente impersonato da InitUser (ad esempio utente `root` che utilizza `su`)		X
ObserverHostName	sn	Nome host del computer che ha inoltrato l'evento al sistema di gestione degli eventi relativi ai dati sulla sicurezza (ad esempio il nome host di un server SysLog). Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
ObserverHostDomain	obsdom	Dominio del computer che ha inoltrato l'evento al sistema di gestione degli eventi relativi ai dati sulla sicurezza (ad esempio il dominio di un server SysLog). Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
ObserverIP	obsip	Indirizzo IP del computer che ha inoltrato l'evento al sistema di gestione degli eventi relativi ai dati sulla sicurezza (ad esempio l'indirizzo IP di un server SysLog). Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		

Campo	Nome breve	Descrizione	Presente in visualizzazione semplice	Presente in visualizzazione dettagliata
ReporterHostName	rn	Nome host del computer che ha segnalato l'evento a un Observer. Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
ReporterHostDomain	repdom	Dominio del computer che ha segnalato l'evento a un Observer. Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
ReporterIP	repip	Indirizzo IP del computer che ha segnalato l'evento a un Observer. Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
SensorType	st	Carattere singolo utilizzato per designare il tipo di sensore (N=rete, H=host, O=sistema operativo, A e I=eventi di revisione di Identity Audit, P=eventi relativi alle prestazioni di Identity Audit). Questo campo può essere utilizzato nelle ricerche, ma non è visualizzato in nessuna delle due visualizzazioni degli eventi.		
DataName	fn	Nome dell'oggetto dati riportato nell'evento (ad esempio il nome del file o il nome della tabella del database).		X
DataContext	rv36	Container dell'oggetto di dati FileName (ad esempio una directory per un file o per un'istanza di database per una tabella di database)		X
TaxonomyLevel1	rv50	Classificazione della destinazione per l'evento. Visualizzato al di sotto del nome dell'evento nel seguente formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel2	rv51	Classificazione della destinazione secondaria per l'evento. Visualizzato al di sotto del nome dell'evento nel seguente formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

Campo	Nome breve	Descrizione	Presente in visualizzazione semplice	Presente in visualizzazione dettagliata
TaxonomyLevel3	rv52	Informazioni sull'azione per l'evento. Visualizzato al di sotto del nome dell'evento nel seguente formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel4	rv53	Informazioni dettagliate per l'evento. Visualizzato al di sotto del nome dell'evento nel seguente formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

Alcuni campi sono tokenizzati. La tokenizzazione dei campi consente di cercare una singola parola al loro interno senza dover utilizzare caratteri jolly. I campi sono tokenizzati in base agli spazi e altri caratteri speciali. In questi campi gli articoli vengono rimossi dall'indice di ricerca.

- EventName
- Message
- ProductName
- FileName
- DataContext
- TaxonomyLevel1
- TaxonomyLevel2
- TaxonomyLevel3
- TaxonomyLevel4

Generazione di rapporti

5

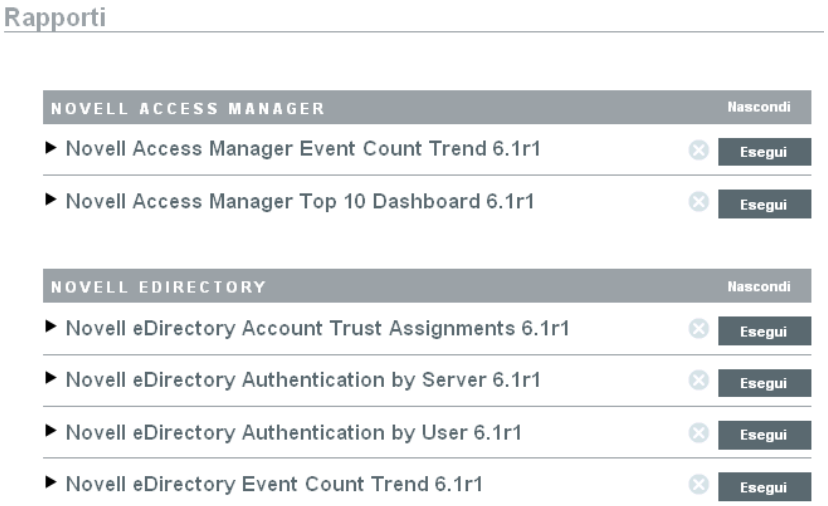
Questo capitolo descrive le procedure per l'esecuzione, la visualizzazione e la gestione di rapporti in Novell® Identity Audit.

5.1 Panoramica

Identity Audit viene installato con un insieme di base di modelli di rapporti correlati ad applicazioni Novell. Tutti gli utenti di Identity Audit possono eseguire rapporti utilizzando i parametri desiderati (ad esempio data di inizio e data di fine) e i risultati dei rapporti possono essere salvati utilizzando nomi personalizzati. Dopo l'esecuzione di un rapporto, tutti gli utenti possono recuperarne i risultati e visualizzarli come file PDF.

I rapporti sono organizzati per categoria. Con Identity Audit vengono installati rapporti per ciascuna origine degli eventi supportata.

Figura 5-1 *Rapporti organizzati per categoria*



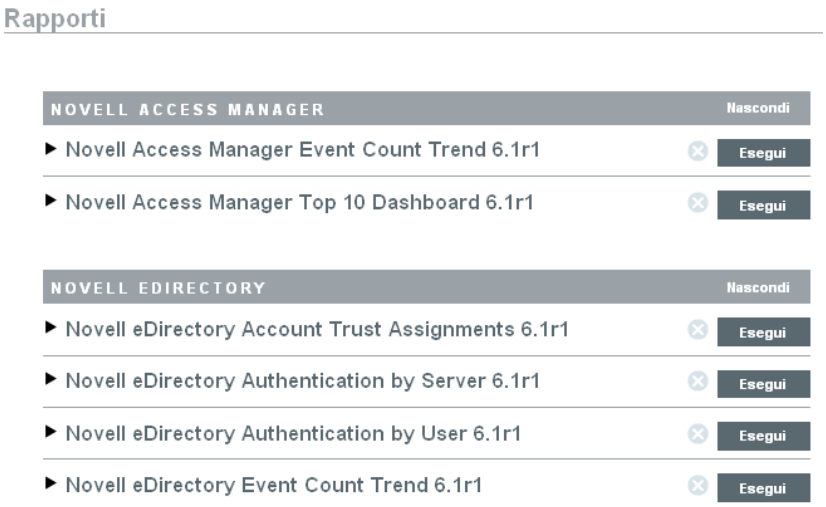
5.2 Esecuzione di rapporti

Con Identity Audit è installata una serie di rapporti organizzata in numerose categorie di prodotti. I rapporti vengono eseguiti in modo asincrono, per permettere agli utenti di continuare a utilizzare l'applicazione durante l'esecuzione. I risultati dei rapporti in formato PDF possono essere visualizzati da tutti gli utenti dopo il completamento dell'esecuzione.

Molte definizioni dei rapporti includono i parametri. All'utente viene richiesto di impostarli prima di eseguire i rapporti. In base al modo in cui lo sviluppatore del rapporto ha progettato il rapporto, i parametri possono essere rappresentati da testo, numeri, valori booleani o date. Un parametro potrebbe avere un valore predefinito o una lista di selezione in base ai valori del database di Identity Audit.

Per eseguire un rapporto:

1 In Identity Audit, fare clic su *Rapporti* per visualizzare i rapporti disponibili.



Se si desidera, fare clic sulla definizione di un rapporto per espanderlo. Se è visualizzato *Sample Report*, è possibile fare clic su *Visualizza* per scoprire l'aspetto di un rapporto completo con una serie di dati di esempio.

2 Selezionare il rapporto desiderato e fare clic su *Esegui*.

3 Impostare la pianificazione per l'esecuzione del rapporto. Se il rapporto verrà eseguito in un secondo momento, sarà anche necessario immettere un'ora di inizio

- Now: è l'impostazione di default. Il rapporto viene eseguito immediatamente.

- Once: questa impostazione consente di eseguire il rapporto una volta, alla data e ora specificate.
- Daily: questa impostazione consente di eseguire il rapporto una volta al giorno all'ora specificata.
- Weekly: questa impostazione consente di eseguire il rapporto una volta alla settimana, nello stesso giorno e all'ora specificata.
- Monthly: questa impostazione consente di eseguire il rapporto lo stesso giorno ogni mese, a partire dalla data e dall'ora specificate. Se, ad esempio, la data e l'ora di inizio sono 28 ottobre alle 14.00, il rapporto verrà eseguito il ventottesimo giorno alle due del pomeriggio di ogni mese.

Nota: tutte le impostazioni dell'ora si basano sull'ora locale del browser.

---

4. Immettere un nome per identificare i risultati del rapporto.

   Non è necessario che il nome del rapporto sia univoco in quanto, per identificare i risultati univocamente, vengono utilizzati anche il nome utente e l'ora.

5. Selezionare la lingua con cui visualizzare il rapporto tra inglese, francese, tedesco, italiano, giapponese, cinese tradizionale, cinese semplificato, spagnolo o portoghese.

6. Selezionare il tipo di rapporto. Tutti i periodi di tempo si basano sull'ora locale del browser.
   - Daily: il rapporto mostra gli eventi dalla mezzanotte del giorno corrente alle 23.59 del giorno corrente. Se l'ora corrente è pari a 8.00, il rapporto mostrerà 8 ore di dati.
   - Weekly: il rapporto mostra gli eventi dalla mezzanotte di domenica della settimana corrente fino alla fine del giorno corrente.
   - Monthly: il rapporto mostra gli eventi dalla mezzanotte del primo giorno del mese corrente fino alla fine del giorno corrente.
   - Custom Date Range: solo per questa impostazione è anche necessario stabilire una data di inizio e una data di fine.
   - Prior Day: il rapporto mostra gli eventi dalla mezzanotte di ieri fino alle 23.59 di ieri.

7. Se è stata selezionata Custom Date Range, impostare la data di inizio (From Date) e la data di fine (To Date) per il rapporto.

   Nota: se viene selezionato Daily, Weekly, Monthly o Prior Day per il tipo di rapporto, queste impostazioni dell'ora vengono ignorate.

   ---

8. Impostare gli eventi Minimum Severity da includere nel rapporto.

9. Impostare gli eventi Maximum Severity da includere nel rapporto.

10. Se il rapporto deve essere inviato a uno o più utenti, immettere gli indirizzi e-mail, separati da virgole.

    Nota: per abilitare l'invio dei rapporti, l'amministratore deve configurare il relay di posta in corrispondenza di *Rules>Configurazione*.

    ---

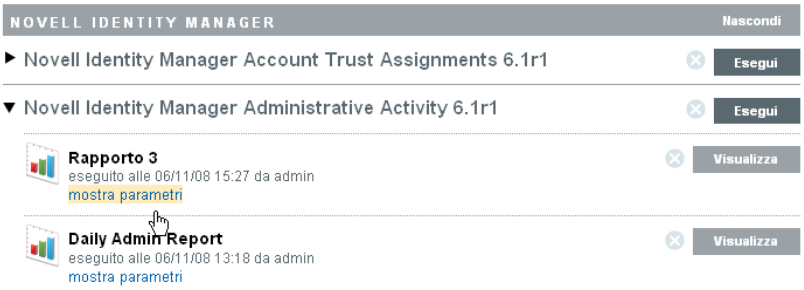
11. Fare clic su *Esegui*.

    Una voce dei risultati del rapporto viene creata e inviata ai destinatari stabiliti.

5.3 Visualizzazione dei rapporti

Gli utenti di Identity Audit possono visualizzare i rapporti nell'applicazione Identity Audit. Altri utenti potrebbero ricevere file `.pdf` dei rapporti tramite e-mail.

1 Per visualizzare l'elenco dei risultati dei rapporti, fare clic su *Visualizza*. I rapporti eseguiti precedentemente vengono visualizzati con il nome personalizzato, l'utente che li ha eseguiti e l'ora di esecuzione.



2 Fare clic su *mostra parametri* per visualizzare i valori esatti utilizzati per l'esecuzione del rapporto.

- Per Report Type, D=Daily, W=Weekly, M=Monthly, DR=Custom Date Range e PD=Prior Day.
- Per Language, en=English, fr=French, de=German, it=Italian, ja=Japanese, pt=Brazilian Portuguese, es=Spanish, zh=Simplified Chinese e zh_TW=Traditional Chinese.

3 Fare clic su *Visualizza* per i risultati dei rapporti da visualizzare. I risultati dei rapporti vengono visualizzati in una nuova finestra informato `.pdf`.

Suggerimento: i risultati dei rapporti sono organizzati dal più recente al più obsoleto.

5.4 Gestione dei rapporti

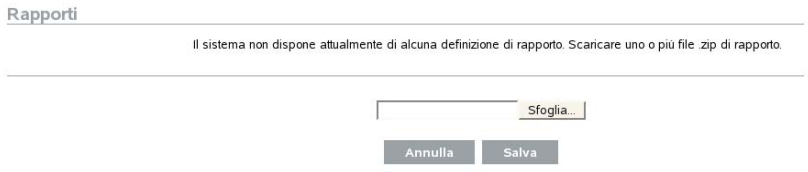
Gli utenti di Identity Audit possono aggiungere, eliminare, aggiornare e pianificare i rapporti.

- Sezione 5.4.1, “Aggiunta di rapporti”, a pagina 39
- Sezione 5.4.2, “Ridenominazione dei risultati dei rapporti”, a pagina 41
- Sezione 5.4.3, “Eliminazione di rapporti”, a pagina 41
- Sezione 5.4.4, “Aggiornamento delle definizioni dei rapporti”, a pagina 41

5.4.1 Aggiunta di rapporti

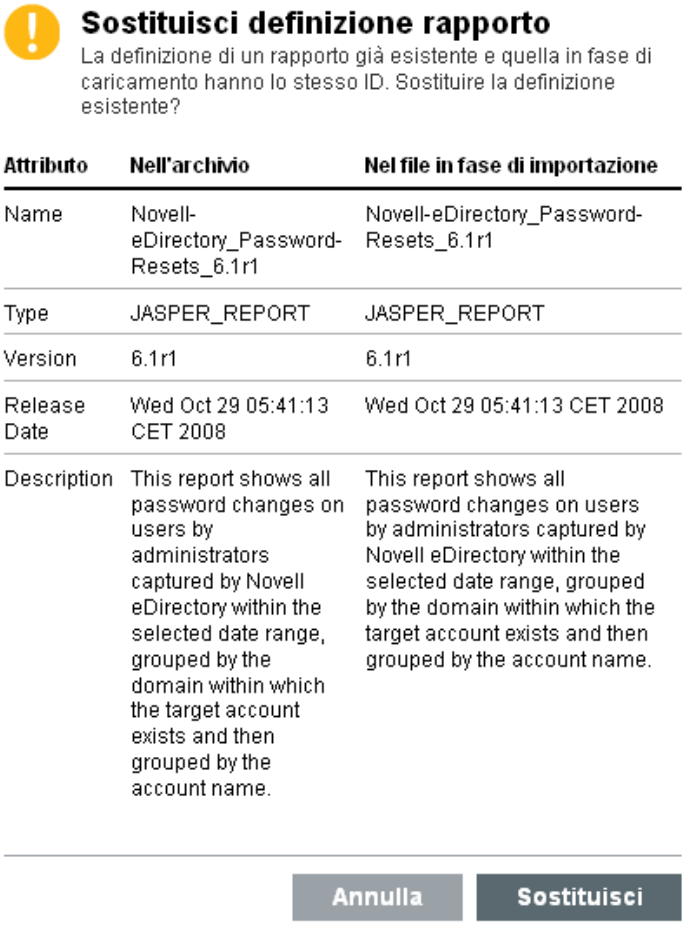
In Identity Audit sono già precaricati i rapporti, ma è possibile caricare nuovi plug-in dei rapporti (file `.zip` speciali che comprendono la definizione di rapporto più i metadati). Se nel sistema non sono presenti rapporti, viene visualizzata la seguente schermata:

Figura 5-2 *Nessun rapporto caricato*



Per aggiungere un rapporto:

1. Fare clic sul pulsante *Rapporti* sul lato sinistro dello schermo.
2. Fare clic sul pulsante *Carica rapporto*.
3. Individuare il percorso del file `.zip` del plug-in del rapporto nel computer locale.
4. Fare clic su *Apri*.
5. Fare clic su *Salva*.
6. Se lo stesso rapporto è già presente nell'archivio dei rapporti (in base all'ID univoco del rapporto), in Identity Audit vengono visualizzati i dettagli del rapporto presente nel sistema e di quello importato. L'utente può decidere se sostituire il rapporto esistente. Nel caso sottostante il rapporto importato ha la stessa versione di quello esistente.



7. La definizione del nuovo rapporto viene aggiunta all'elenco in ordine alfabetico e, se necessario, il rapporto può essere eseguito immediatamente.

Download di rapporti nuovi o aggiornati

I rapporti nuovi o aggiornati da Novell possono essere scaricati dal sito Web dei contenuti di Novell (http://support.novell.com/products/identityaudit/identityaudit10.html).

Creazione di nuovi rapporti

Gli utenti possono modificare o scrivere rapporti mediante iReport di JasperForge*, uno strumento grafico di creazione di rapporti per i rapporti Jasper. iReport è uno strumento di sviluppo di rapporti open source disponibile per il download dal sito JasperForge.org (http://jasperforge.org/plugins/project/project_home.php?group_id=83) (al momento della pubblicazione della presente documentazione).

I rapporti nuovi o modificati possono includere ulteriori campi di database che non sono presenti nell'interfaccia Web di Identity Audit, che devono aderire ai requisiti di file e formato dei plug-in dei rapporti. Per ulteriori informazioni sui campi del database e sui requisiti di file e formato per i plug-in dei rapporti, vedere il sito Web di Sentinel SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

5.4.2 Ridenominazione dei risultati dei rapporti

I risultati dei rapporti, ma non le definizioni dei rapporti, possono essere ridenominati nell'interfaccia di Identity Audit.

1. Fare clic sul pulsante *Rapporti* sul lato sinistro dello schermo.
2. Fare clic sul nome di un rapporto per espanderlo.
3. Fare clic sul nome dei risultati del rapporto da ridenominare.
4. Immettere il nuovo nome.
5. Fare clic su *Rinomina*.

5.4.3 Eliminazione di rapporti

È possibile eliminare un insieme di risultati dei rapporti oppure la definizione di un rapporto. Se si elimina la definizione di un rapporto, vengono eliminati tutti i risultati a essa correlati.

Se si elimina un rapporto la cui esecuzione è in corso, viene annullata l'interrogazione del database.

5.4.4 Aggiornamento delle definizioni dei rapporti

Gli utenti possono caricare i rapporti aggiornati in Identity Audit per sostituire un rapporto esistente. Per ulteriori informazioni, vedere la Sezione 5.4.1, “Aggiunta di rapporti”, a pagina 39.

Raccolta dei dati

6

Gli amministratori possono configurare e monitorare la raccolta di dati per Novell® Identity Audit. Identity Audit consente di raccogliere dati da varie applicazioni Novell mediante Platform Agent di Novell Audit. Per ulteriori informazioni sulle versioni supportate di Platform Agent, vedere la Sezione 2.4, “Platform Agent supportato”, a pagina 14.

6.1 Configurazione delle origini degli eventi

Anche se Identity Audit è preconfigurato per accettare dati da molte applicazioni Novell, i server delle applicazioni stessi (origini degli eventi) devono essere configurati per l'invio dei dati al server di Identity Audit. Questo processo è parte dell'installazione semplice di Identity Audit. Per ulteriori informazioni, consultare laSezione 3.2, “Configurazione delle origini degli eventi”, a pagina 20.

6.2 Stato della raccolta dei dati

Gli amministratori possono abilitare o disabilitare la raccolta dei dati in modo globale o in base all'applicazione. Possono anche visualizzare informazioni sull'integrità di ciascuna applicazione.

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic su *Raccolta* nell'angolo superiore destro della pagina.

3 Abilitare o disabilitare la raccolta globale dei dati dal server di Audit.

4 Abilitare o disabilitare la raccolta di dati specifici dell'applicazione dalle origini degli eventi.

5 Fare clic su *mostra dettagli* per visualizzare ulteriori informazioni sulle connessioni attive per ogni applicazione.

Le modifiche a questa pagina hanno effetto immediato.

- Sezione 6.2.1, “Server Audit”, a pagina 44
- Sezione 6.2.2, “Origini degli eventi”, a pagina 44

6.2.1 Server Audit

Nella sezione *Server Audit* gli amministratori possono abilitare o disabilitare la raccolta di dati a livello globale mediante le opzioni On e Off. Viene anche visualizzato lo stato di integrità del server Audit.

Healthy: un indicatore di colore verde rappresenta l'integrità del server Audit, il che significa che è acceso, è in attesa su una porta e non presente alcun errore irrisolto.

Errore: un indicatore di colore rosso significa che nel server Audit si è verificato un errore. Per ulteriori informazioni visualizzare i file `server0.*.log`.

Offline: un indicatore di colore grigio significa che un amministratore ha attivato la modalità non in linea del server Audit.

6.2.2 Origini degli eventi

Nella sezione *Event Sources* gli amministratori possono attivare la raccolta di dati a livello di applicazione. Queste impostazioni possono influire sulla raccolta di dati per numerosi server (ad esempio più istanze di eDirectory).

Nota: queste impostazioni consentono di abilitare, o disabilitare, la raccolta di dati di Identity Audit dalle applicazioni elencate. Non permettono di avviare o interrompere i servizi nei computer delle origini degli eventi.

Lo stato di integrità per ogni icona è indicato da un'icona di colore rosso, giallo, verde o nero. Per la maggior parte degli stati è possibile visualizzare ulteriori informazioni facendo clic su *mostra dettagli*.

Healthy: un indicatore di colore verde significa che l'origine dell'evento è integra e che Identity Audit ha ricevuti i dati da essa.

Avviso: un indicatore di colore giallo indica una condizione di avviso. Una causa frequente riguarda il fatto che l'applicazione è attiva in Identity Audit, ma non ha inviato alcun dato. Ciò potrebbe, ad esempio, accadere se Platform Agent nell'origine dell'evento non è configurato in modo corretto per l'invio dei dati a Identity Audit o se la registrazione non è abilitata per l'applicazione. Fare clic su *mostra dettagli* per ulteriori informazioni.

Errore: un indicatore di colore rosso significa che il server di Identity Audit segnala un errore di connessione o di ricezione dei dati da questa applicazione. Fare clic su *mostra dettagli* per ulteriori informazioni.

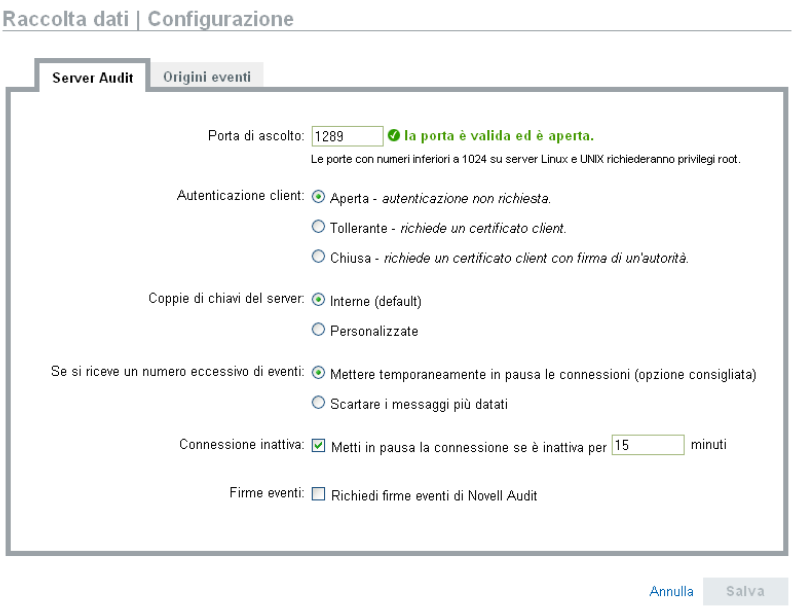
Offline: un indicatore di colore grigio significa che l'origine dell'evento è stata disattivata. Identity Audit non elabora alcun dato.

Per ogni origine dati online, Identity Audit mostra la frequenza di eventi calcolata per gli eventi in entrata. La frequenza di eventi viene ricalcolata ogni 60 secondi.

6.3 Opzioni del server Audit

Gli amministratori possono modificare alcune impostazioni relative al modo in cui Identity Audit rimane in attesa di dati provenienti dalle applicazioni di origine degli eventi, inclusa la porta su cui Identity Audit è in attesa e il tipo di autenticazione fra l'origine dell'evento e Identity Audit.

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic sul collegamento *Raccolta* situato nella parte superiore dello schermo.
3. Fare clic sul collegamento *Configurazione* nella parte destra dello schermo.
4. Accertarsi che *Server Audit* sia selezionato.



5. Immettere la porta in cui il server di Identity Audit rimarrà in attesa dei messaggi dalle origini degli eventi. Per ulteriori informazioni, vedere la Sezione 6.3.1, “Configurazione della porta e inoltro della porta”, a pagina 46.
6. Configurare le impostazioni dell'autenticazione del client e delle coppie di chiavi del server appropriate. Per ulteriori informazioni, vedere la Sezione 6.3.2, “Autenticazione client”, a pagina 47.
7. Selezionare il comportamento del server di Identity Audit quando il buffer contiene troppi eventi.

   Temporarily pause connections: questa impostazione interrompe le connessioni esistenti e l'accettazione di nuove connessioni finché il buffer dispone di spazio per i nuovi messaggi. Nel frattempo i messaggi vengono memorizzati nella cache dalle origini degli eventi.

Drop oldest messages: questa impostazione rimuove i messaggi più vecchi per accettare i nuovi messaggi.

Avviso: non esiste alcun metodo supportato per ripristinare i messaggi rimossi se si seleziona *Drop oldest messages*.

---

8 Selezionare *Idle Connection* per disconnettere le origini degli eventi che non hanno inviato dati per un determinato periodo di tempo.

Le connessioni delle origini degli eventi verranno ricreate automaticamente al momento del nuovo invio dei dati.

9 Immettere il numero di minuti prima che una connessione inattiva venga disconnessa.

10 Selezionare *Event Signatures* per ricevere una firma con l'evento.

Nota: per ricevere una firma, Platform Agent nell'origine dell'evento deve essere configurato in modo corretto. Per ulteriori informazioni, vedere la Sezione 6.1, “Configurazione delle origini degli eventi”, a pagina 43.

---

11 Fare clic su *Salva*.

6.3.1 Configurazione della porta e inoltro della porta

La porta di default su cui Identity Audit è in attesa di messaggi provenienti da Platform Agent è la porta 1289. Quando questa porta viene impostata, il sistema verifica che la porta sia valida e che sia aperta.

L'associazione a porte inferiori alla 1024 richiede privilegi da utente root. Al contrario Novell consiglia di utilizzare una porta superiore alla 1024. È possibile modificare i dispositivi di origine per l'invio a una porta superiore o l'utilizzo dell'inoltro della porta nel server di Identity Audit.

Per modificare l'origine dell'evento per l'invio a una porta diversa:

1 Effettuare il login al computer delle origini degli eventi.

2 Aprire il file `logevent` per la modifica. Il file si trova in un'ubicazione diversa in base al sistema operativo:

- Linux: `/etc/logevent.conf`
- Windows: `C:\WINDOWS\logevent.cfg`
- NetWare: `SYS:\etc\logevent.cfg`
- Solaris: `/etc/logevent.conf`

3 Impostare il parametro LogEnginePort sulla porta desiderata.

4 Salvare il file.

5 Riavviare Platform Agent. Il metodo varia in base al sistema operativo e all'applicazione. Riavviare il computer o fare riferimento alla documentazione specifica dell'applicazione nel sito Web di documentazione di Novell (http://www.novell.com/documentation) per ulteriori informazioni.

Per configurare l'inoltro della porta nel server di Identity Audit:

1 Effettuare il login al sistema operativo del server di Identity Audit come utente `root`, o `su` per l'utente `root`.

2 Aprire il file `/etc/init.d/boot.local` per la modifica.

3 Aggiungere il comando riportato di seguito accanto alla fine del processo di avvio:

```
iptables -A PREROUTING -t nat -p protocol --dport incoming port -j
DNAT --to-destination IP:rerouted port
```

dove *protocol* è tcp o udp, *incoming port* è la porta in cui arrivano i messaggi e *IP:rerouted port* rappresenta l'indirizzo IP del computer locale e una porta disponibile superiore alla 1024.

4 Salvare le modifiche.

5 Riavviare. Se non è possibile riavviare subito, eseguire il comando `iptables` precedente da una riga di comando.

6.3.2 Autenticazione client

Le origini degli eventi inviano i dati attraverso una connessione SSL e l'impostazione *Client authentication* per il server di Identity Audit determina il tipo di autenticazione eseguita per i certificati provenienti da Platform Agent nelle origini degli eventi.

Aperta: non è richiesta l'autenticazione. Identity Audit non richiede o convalida un certificato per l'origine degli eventi.

Tollerante: è richiesto un certificato X.509 valido per l'origine degli eventi, ma il certificato non viene convalidato. Non è necessario che il certificato sia firmato da un'autorità di certificazione.

Chiusa: è richiesto un certificato X.509 valido per l'origine degli eventi e deve essere firmato da un'autorità di certificazione attendibile. Se l'origine degli eventi non presenta un certificato valido, Identity Audit non accetterà i dati degli eventi corrispondenti.

- “Creazione di un truststore” a pagina 47
- “Importazione di un truststore” a pagina 48
- “Coppia di chiavi del server” a pagina 49

Creazione di un truststore

Per un'autenticazione chiusa è necessario disporre di un truststore che contenga il certificato dell'origine dell'evento o il certificato per l'autorità di certificazione che ha firmato il certificato dell'origine dell'evento. Quando si dispone di un certificato DER o PEM, è possibile creare il truststore mediante l'utility CreateTruststore disponibile con Identity Audit.

1 Effettuare il login al server di Identity Audit come utente novell.

2 Individuare `/opt/novell/identity_audit_1.0_x86/data/updates/done`.

3 Decomprimere il file `audit_connector.zip`.

```
unzip audit_connector.zip
```

4 Copiare `TruststoreCreator.sh` o `TruststoreCreator.bat` nel computer con i certificati o copiare i certificati nel computer con l'utility TruststoreCreator.

5 Eseguire l'utility `TruststoreCreator.sh`.

```
TruststoreCreator.sh -keystore /tmp/my.keystore -password
password1 -certs /tmp/cert1.pem,/tmp/cert2.pem
```

In questo esempio l'utility TruststoreCreator crea un file di archivio chiavi denominato `my.keystore` contenente due certificati, vale a dire `cert1.pem` e `cert2.pem`. Il file è protetto dalla password *password1*.

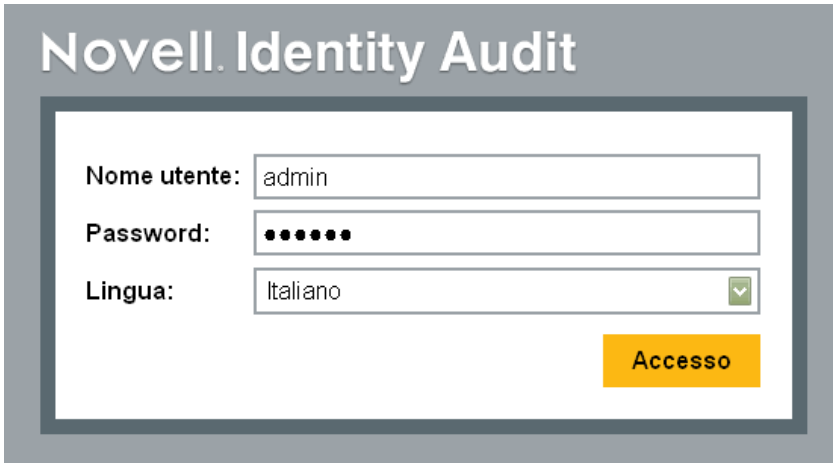
Importazione di un truststore

Per un'autenticazione chiusa l'amministratore può importare un truststore mediante il pulsante *Import*. Ciò consente di garantire che solo le origini degli eventi autorizzate inviino dati a Identity Audit. Il truststore deve includere il certificato dell'origine dell'evento o il certificato dell'autorità di certificazione che lo ha firmato.

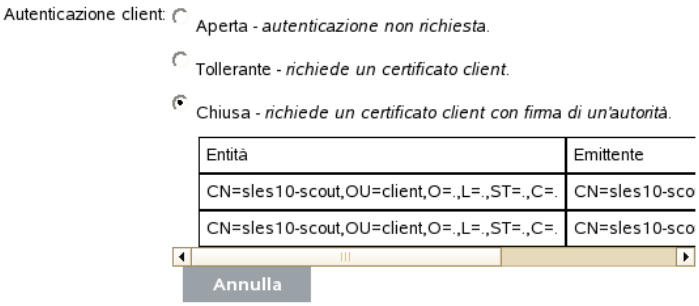
La procedura riportata di seguito deve essere eseguita nel computer che dispone del truststore. È possibile aprire un browser Web nel computer con il truststore o spostare il truststore in qualsiasi computer con un browser Web.

Per importare un truststore:

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic sul collegamento *Raccolta* situato nella parte superiore dello schermo.
3. Fare clic sul collegamento *Configurazione* nella parte destra dello schermo.
4. Assicurarsi che la scheda *Server Audit* sia selezionata.
5. Selezionare l'opzione *Chiusa* in corrispondenza di *Client authentication*.



6. Fare clic su *Browse* e individuare il file truststore, ad esempio `my.keystore`.
7. Immettere la password per il file truststore.
8. Fare clic su *Importa*.
9. Fare clic su *Dettagli* per ulteriori informazioni sul truststore.



10 Fare clic su *Salva*.

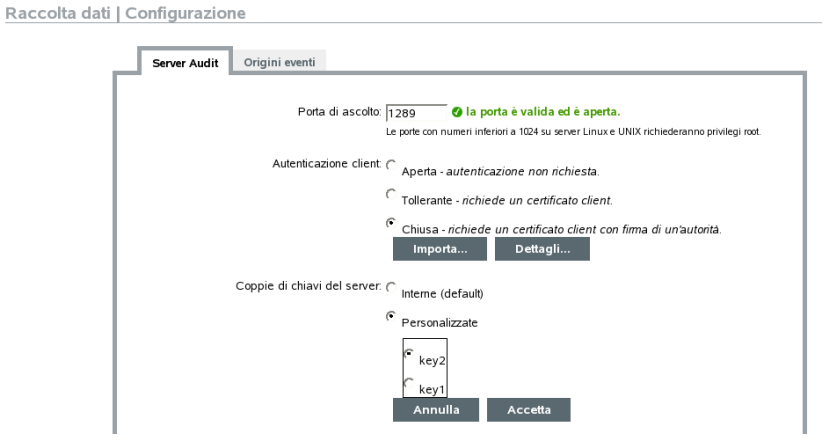
Dopo l'importazione del truststore, è possibile fare clic su *Dettagli* per visualizzare il certificato incluso nel truststore.

Coppia di chiavi del server

Identity Audit viene installato con un certificato incorporato, utilizzato per autenticare il server di Identity Audit nelle origini degli eventi. Questo certificato può essere sostituito con un certificato firmato da un'autorità di certificazione pubblica.

Per sostituire il certificato incorporato.

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic sul collegamento *Raccolta* situato nella parte superiore dello schermo.
3. Fare clic sul collegamento *Configurazione* nella parte destra dello schermo.
4. Accertarsi che *Server Audit* sia selezionato.
5. In *Server key pairs* selezionare *Personalizzato*.
6. Fare clic su *Browse* e individuare il file truststore.
7. Immettere la password per il file truststore.
8. Fare clic su *Importa*.



Se esiste più di una coppia di chiavi pubblica-privata nel file, selezionare la coppia di chiavi desiderata e fare clic su *OK*.

9 Fare clic su *Dettagli* per ulteriori informazioni sulla coppia di chiavi del server.

10 Fare clic su *Salva*.

6.4 Origini degli eventi

La pagina *Event Sources* consente agli amministratori di configurare in che modo viene determinato il tempo per gli eventi da ciascuna origine dell'evento. L'ora dell'evento può essere basata sulla registrazione dell'orario dall'origine dell'evento ("Considera affidabile l'ora dell'evento") o sulla registrazione dell'orario dal server di Identity Audit. La registrazione dell'orario influisce sull'ordine in cui gli eventi vengono visualizzati in una ricerca se si effettua l'ordine in base all'ora. La registrazione dell'orario influisce anche sull'ora visualizzata nei rapporti. Il valore di default è l'ora del server di Identity Audit.

Nota: si consiglia di utilizzare un server NTP per sincronizzare l'ora su tutti i computer presenti nel sistema di Identity Audit. Se è disponibile un server NTP, è consigliabile fare affidamento sull'ora dell'evento per le applicazioni. Se un server NTP non è disponibile, è consigliabile utilizzare l'ora del server di Identity Audit per tutte le applicazioni, vale a dire l'impostazione di default, per correggere tutte le differenze di ora tra i computer.

Per modificare le opzioni relative all'ora degli eventi:

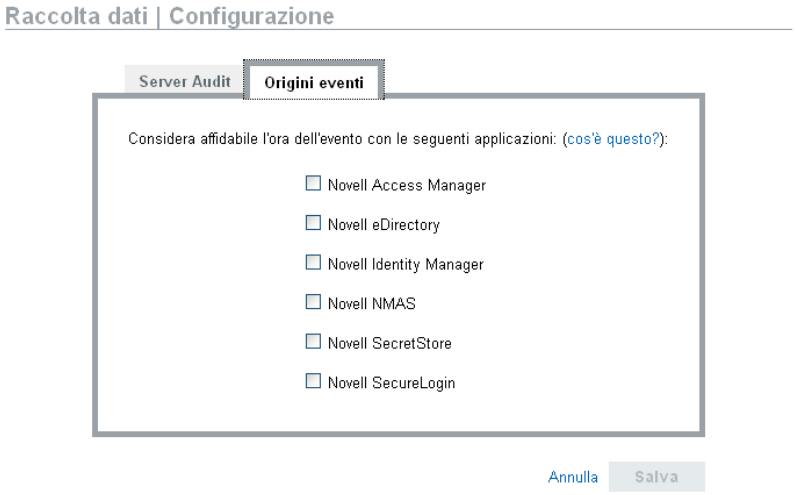
1 Eseguire il login a Identity Audit come amministratore.

2 Fare clic sul collegamento *Raccolta* situato nella parte superiore dello schermo.

3 Fare clic sul collegamento *Configurazione* nella parte destra dello schermo.

4 Fare clic su *Event Source*.

5 Selezionare le applicazioni per le quali Identity Audit dovrà utilizzare la registrazione dell'ora degli eventi dell'applicazione di origine.



In tutti gli altri casi la registrazione dell'ora del server di Identity Audit sostituisce quella dell'applicazione originale.

Le modifiche hanno effetto immediato su tutti i nuovi eventi in entrata. È possibile che l'elaborazione degli eventi già presenti nella coda richieda qualche istante.

Archiviazione dei dati 7

Durante l'installazione di Novell® Identity Audit viene installato un database PostgreSQL contenente tutte le tabelle e tutti gli utenti necessari per l'esecuzione di Identity Audit. Il database include inoltre stored procedure progettate per la gestione delle partizioni del database e per l'archiviazione dei dati obsoleti. Le impostazioni di archiviazione possono essere gestite dagli amministratori mediante l'interfaccia Web.

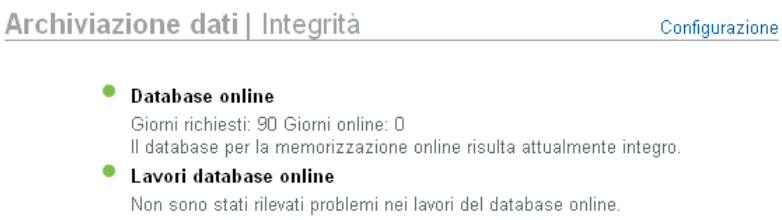
7.1 Integrità del database

La pagina Archiviazione dati | Integrità, disponibile solo per gli amministratori, mostra le informazioni relative all'integrità del database in base al numero di partizioni disponibili nel database e al numero di operazioni riuscite di creazione di nuove partizioni e di archiviazione dei dati da parte delle stored procedure (se configurate).

Per visualizzare le informazioni sull'integrità del database:

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic sul collegamento Archiviazione situato in alto a sinistra nella pagina.

   Viene visualizzata la pagina contenente le informazioni sull'integrità.



In questa pagina è possibile verificare se varie funzioni del database hanno uno stato di integrità (verde), di avviso (giallo) o di errore (rosso).

Database online: questo indicatore mostra se nel database è presente il numero previsto di partizioni per ciascuna tabella partizionata.. Tale numero è basato sul numero di giorni in cui il database è configurato per essere online o sul numero di giorni a partire dall'installazione, se si tratta di una nuova installazione.

Se il numero di partizioni non corrisponde a quello previsto, nella pagina viene visualizzato il nome della tabella, il numero di partizioni previste e il numero di partizioni effettive presenti nel database.

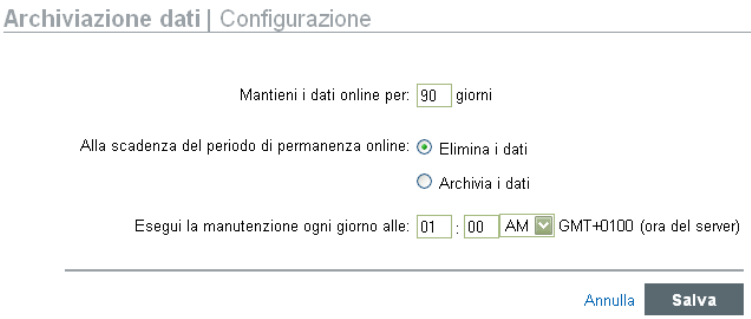
Lavori database online: questo indicatore diventa rosso se si sono verificati errori durante l'ultima esecuzione delle stored procedure per aggiungere partizioni ed eliminare i dati. Se l'archiviazione è abilitata, questo indicatore mostra solo se si sono verificati errori durante l'ultima esecuzione del lavoro per aggiungere le partizioni. Se ci sono errori, la pagina visualizza il nome, la registrazione dell'orario e i dettagli associati al lavoro non andato a buon fine.

Archivia database: questo indicatore viene visualizzato solo se l'archiviazione è abilitata. Diventa rosso se si sono verificati errori durante l'ultima esecuzione della stored procedure per l'archiviazione dei dati. Se ci sono errori, la pagina visualizza il nome, la registrazione dell'orario e i dettagli associati al lavoro non andato a buon fine.

7.2 Configurazione dell'archiviazione dati

Il database costituisce l'archivio per gli eventi in entrata, per le informazioni di configurazione e per i risultati dei rapporti. Identity Audit fornisce procedure per la gestione del database allo scopo di impedire che lo spazio del database si esaurisca. La pagina Archiviazione dati, accessibile solo agli amministratori, consente di configurare vari aspetti dell'archiviazione dati.

Figura 7-1 *Configurazione dell'archiviazione dati*



Keep data online for: gli amministratori possono specificare il numero di giorni in cui i dati verranno mantenuti nel database per la creazione dei rapporti. La durata minima è pari a un giorno e il numero deve essere un intero (senza decimali).

After online period expires: alla scadenza del periodo di conservazione online tutti i dati degli eventi più vecchi del periodo di tempo indicato vengono eliminati o spostati all'esterno del database in una directory di archiviazione.

Avviso: Novell non supporta il recupero dei dati eliminati, quindi selezionare l'opzione Delete con attenzione.

Archive to this database directory: se si è selezionata l'opzione *Archivia i dati*, specificare il percorso di una directory esistente in cui verranno salvati i dati archiviati. L'utente novell deve disporre delle autorizzazioni di scrittura per la directory, che deve essere già esistente. Per default, il percorso è impostato sulla directory /data/db_archive della home directory di Identity Audit. La directory di default viene creata con le autorizzazioni appropriate durante l'installazione di Identity Audit.

Importante: per evitare che lo spazio sul disco rigido si esaurisca, si consiglia di spostare periodicamente i file degli archivi in un'ubicazione per l'archiviazione a lungo termine.

Test: se viene selezionata l'opzione *Archivia i dati*, il pulsante Test consente di verificare se la directory di archiviazione esiste e se l'utente novell dispone delle autorizzazioni di scrittura.

Perform maintenance every day at: specificare l'orario in cui dovranno essere eseguite le routine di manutenzione. L'orario è basato sull'ora locale del server di Identity Audit. Una stored procedure viene eseguita all'ora pianificata per la manutenzione allo scopo di aggiungere partizioni al database. Dopo due ore, viene eseguita una stored procedure per archiviare o eliminare i dati precedenti alla scadenza configurata.

È consigliabile pianificare l'archiviazione dei dati per un'ora del giorno in cui il livello di utilizzo del database è relativamente basso.

Regole

8

Questo capitolo descrive i canali utilizzabili per l'invio degli eventi da Identity Audit a un altro sistema.

8.1 Panoramica sulle regole

L'interfaccia delle regole fornisce la capacità di definire le regole per valutare tutti gli eventi in entrata e distribuire gli eventi selezionati ai canali di output designati. Ad esempio ogni evento di gravità 5 può essere inviato via e-mail a una lista di distribuzione di analisti della sicurezza o a un amministratore.

Nota: tutti gli eventi vengono inoltre distribuiti al database.

Un evento in entrata viene valutato in relazione a ogni regola di filtraggio fino a trovare una corrispondenza, poi vengono eseguite le azioni di distribuzione associate a tale regola:

Invia un'e-mail: consente di inviare l'evento a uno o più utenti mediante un relay SMTP configurato.

Registra su file: l'evento viene salvato sul file specificato nel server di Identity Audit.

Registra in SysLog: l'evento viene inoltrato al server SysLog configurato.

Suggerimento: gli eventi vengono elaborati dalle azioni associate una per volta. È quindi consigliabile prendere in considerazione le implicazioni sulle prestazioni durante la selezione del canale di output a cui sono inviati gli eventi. Ad esempio, l'azione Registra su file è quella che richiede meno risorse, pertanto può essere utilizzata per verificare i criteri della regola per determinare il volume dei dati prima di inviare una serie di eventi tramite e-mail o SysLog.

Inoltre, quando si imposta l'azione Invia un'e-mail, si dovrebbe prendere in considerazione il numero di eventi che il destinatario è effettivamente in grado di gestire e adattare il filtro in base alla regola.

L'output dell'evento è in JSON (JavaScript Object Notation), vale a dire un formato di scambio dati a bassa densità. Gli eventi sono costituiti da nomi dei campi (come "evt" per EventName), seguiti da due punti e da un valore (come "Start"), separati da virgole.


```
{"st":"I","evt":"Start","sev":"1","sres":"Collector","res":"Collec
torManager","rv99":"0","rv1":"0","repassetid":"0","rv77":"0","agen
t":"Novell SecureLogin","obsassetid":"0","vul":"0","port":"Novell
SecureLogin","msg":"Processing started for Collector Novell
SecureLogin (ID D892E9F0-3CA7-102B-B5A1-
005056C00005).","dt":"1224204655689","id":"751D97B0-7E13-112B-
B933-000C29E8CEDE","src":"D892E9F0-3CA7-102B-B5A2-005056C00004"}
```

8.2 Configurazione delle regole

È possibile configurare le regole di Identity Audit per filtrare gli eventi in base a uno o più campi utilizzabili per le ricerche. Per un elenco dei campi evento di Identity Audit su cui è possibile eseguire delle ricerche vedere la Tabella 4-1 a pagina 30. Ogni regola può essere associata a una o più azioni configurate.

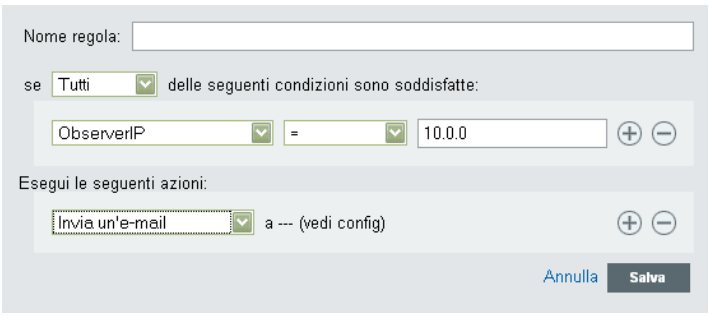
8.2.1 Criteri dei filtri

Le regole possono essere basate su qualsiasi campo evento in cui è possibile eseguire delle ricerche. Per un elenco di questi campi, vedere la Tabella 4-1 a pagina 30. Gli operatori disponibili dipendono dal tipo di dati del campo evento. Ad esempio `match subnet` è disponibile per gli indirizzi IP e `match regex` è disponibile per i campi di testo.

8.2.2 Aggiunta di una regola

Gli amministratori possono aggiungere una regola basata sul filtro e definire uno o più canali a cui inviare gli eventi che soddisfano i criteri della regola.

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic su *Rules* nell'angolo superiore sinistro della pagina.
3. Fare clic su *Add Rule*.
4. Immettere il nome della regola.
5. Se verranno create più condizioni, selezionare *All* per unire le condizioni con un operatore AND. Selezionare *Any* per unire le condizione con un operatore OR.
6. Selezionare il campo evento, l'operatore e il valore per il filtro.



7. Selezionare un'azione che verrà eseguita in ogni evento che soddisfa i criteri del filtro.

   I dettagli dell'azione si basano sulle informazioni di configurazione visualizzate se si fa clic sul collegamento *Configurazione*.

8 Configurare ulteriori azioni, come desiderato.

9 Fare clic su *Salva*.

8.2.3 Ordinare le regole

Dato che gli eventi vengono valutati in base alle regole fino a trovare una corrispondenza, è consigliabile ordinare le regole di conseguenza. Le regole definite con maggiore restrizione e le regole più importanti devono essere collocate all'inizio dell'elenco. Quando esiste più di una regola, le regole possono essere riordinate mediante il trascinamento.

Per riordinare le regole:

1 Eseguire il login a Identity Audit come amministratore.

2 Fare clic su *Rules* nell'angolo superiore destro della pagina.

3 Posizionare il puntatore del mouse sull'icona a sinistra della numerazione delle regole per abilitare il trascinamento. Il cursore cambia forma.

4 Trascinare la regola nella posizione corretta nell'elenco ordinato.

8.2.4 Eliminazione di una regola

Quando si elimina una regola, se nella coda sono presenti eventi associati a una o più azioni, è possibile che lo svuotamento della coda successivo alla disattivazione della regola richieda del tempo.

8.2.5 Attivazione o disattivazione di una regola

A sinistra di ciascuna regola, in una colonna intestata On, è presente una casella di controllo per attivare tale regola. Le nuove regole sono attivate per default. Se si disattiva una regola, gli eventi in entrata non verranno più valutati in base a quella regola. Se nella coda sono presenti eventi associati a una o più azioni, è possibile che lo svuotamento della coda successivo alla disattivazione della regola richieda del tempo.

8.3 Configurazione di azioni

Un evento viene distribuito a uno o più canali quando soddisfa i criteri specificati da una delle regole. Prima che gli eventi possano essere inviati a un canale, l'azione per l'invio a tale canale deve essere configurata con le informazioni di connessione appropriate e le credenziali di autenticazione,

se necessario per il relay SMTP. Il sistema di Identity Audit consente la configurazione di una sola connessione per tipo di azione. Ad esempio, tutti gli eventi che vengono registrati in un file devono essere registrati nello stesso file.

- Sezione 8.3.1, “Invia un'e-mail”, a pagina 60
- Sezione 8.3.2, “Registrazione in SysLog”, a pagina 61
- Sezione 8.3.3, “Registrazione su file”, a pagina 61

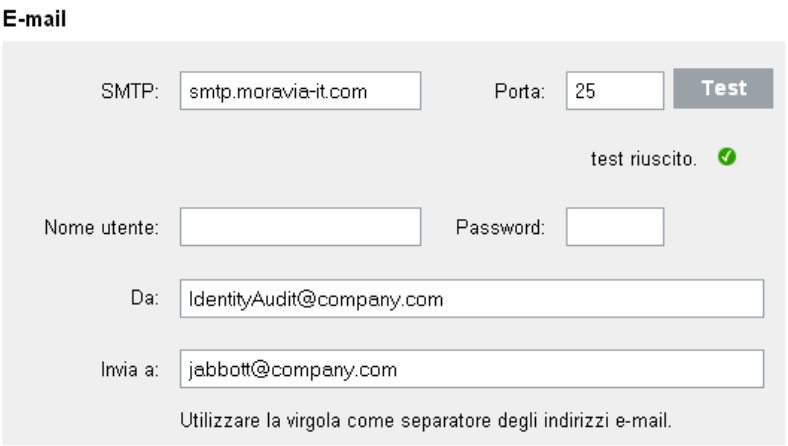
8.3.1 Invia un'e-mail

Per configurare l'azione Invia un'e-mail, è necessario disporre delle informazioni relative al relay SMTP (indirizzo IP e numero della porta), nonché conoscere gli indirizzi del mittente e del destinatario. Per inviare l'e-mail a più di un indirizzo è possibile specificare un elenco di indirizzi separati dalla virgola.

Nota: per evitare di sovraccaricare il relay SMTP o i destinatari dell'e-mail, questa azione deve essere utilizzata solo con regole che generano un volume di eventi ridotto.

Questa configurazione del relay SMTP viene utilizzata anche per inviare i rapporti agli utenti.

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic su *Rules* nell'angolo superiore destro della pagina.
3. Fare clic su *Configurazione*.
4. In corrispondenza di *e-mail* immettere il nome e la porta di un relay SMTP disponibile. Se si desidera, fare clic su *Test* per verificare la connessione.



5. Se il relay SMTP richiede l'autenticazione, immettere nome utente e password.
6. Immettere un indirizzo da cui proverranno i messaggi e-mail.
7. Immettere uno o più indirizzi e-mail, separati da virgole.
8. Fare clic su *Salva*.

Tutti gli eventi di Identity Audit che soddisfano i criteri di un filtro per cui è stata definita un'azione Invia un'e-mail vengono inviati allo stesso relay SMTP e allo stesso insieme di indirizzi.

8.3.2 Registrazione in SysLog

Per configurare l'azione Registra in SysLog, sono necessarie informazioni sulla connessione per il server SysLog (indirizzo IP e numero di porta).

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic su *Rules* nell'angolo superiore destro della pagina.
3. Fare clic su *Configurazione*.
4. In corrispondenza di *Syslog* immettere un nome o un indirizzo IP e aprire la porta di un server SysLog. Se si desidera, fare clic su *Test* per verificare che il server di destinazione e la porta esistano.

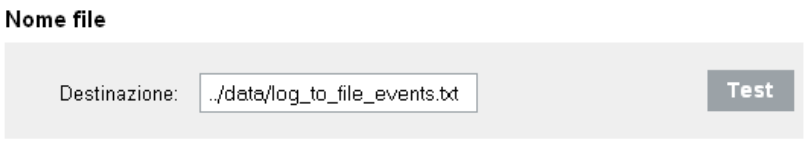
5. Fare clic su *Salva*.

Tutti gli eventi di Identity Audit che soddisfano i criteri di un filtro per cui è stata definita un'azione Registra in SysLog vengono inviati allo stesso server SysLog.

8.3.3 Registrazione su file

Per configurare l'azione Registra su file è necessario conoscere il percorso e il nome del file in cui verranno salvati gli eventi. L'utente novell deve disporre delle autorizzazioni di scrittura per la directory, che deve essere già esistente. Se il file non esiste, Identity Audit ne creerà uno.

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic su *Rules* nell'angolo superiore destro della pagina.
3. Fare clic su *Configurazione*.
4. In corrispondenza di *Filename* immettere il percorso del file in cui devono essere scritti gli eventi. Se si desidera, fare clic su *Test* per verificare la connessione.



5. Fare clic su *Salva*.

Tutti gli eventi di Identity Audit che soddisfano i criteri di un filtro per cui è stata definita un'azione Registra su file vengono registrati nello stesso file.

Amministrazione degli utenti

9

In Novell® Identity Audit gli amministratori possono aggiungere, modificare ed eliminare utenti, nonché concedere diritti amministrativi. Gli utenti possono modificare i dettagli del proprio profilo.

9.1 Aggiunta di un utente

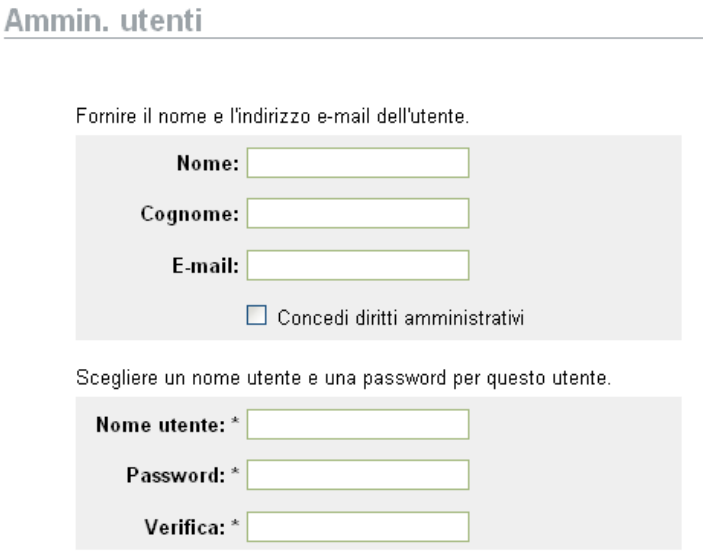
Mediante l'aggiunta di un utente al sistema di Identity Audit viene creato un utente dell'applicazione che successivamente può eseguire il login all'applicazione Identity Audit.

Se si seleziona l'opzione *Grant administrative rights*, all'utente vengono concessi diritti amministrativi per il sistema di Identity Audit. I diritti amministrativi comprendono la capacità di gestire le seguenti funzioni:

- Amministrazione degli utenti
- Raccolta dei dati
- Archiviazione dei dati

Per aggiungere un utente:

1. Eseguire il login a Identity Audit come amministratore.
2. Fare clic su *User Admin* nell'angolo superiore destro della pagina.
3. Fare clic su *Add a user*.
4. Immettere le informazioni sull'utente.



I campi con un asterisco (*) sono obbligatori e il nome utente deve essere univoco.

Nota: il formato dell'indirizzo e-mail viene convalidato, ma i campi del numero telefonico consentono qualsiasi formato. Assicurarsi di immettere un numero di telefono valido.

5 Selezionare *Grant administrative rights*, se si desidera.

6 Fare clic su *Salva*.

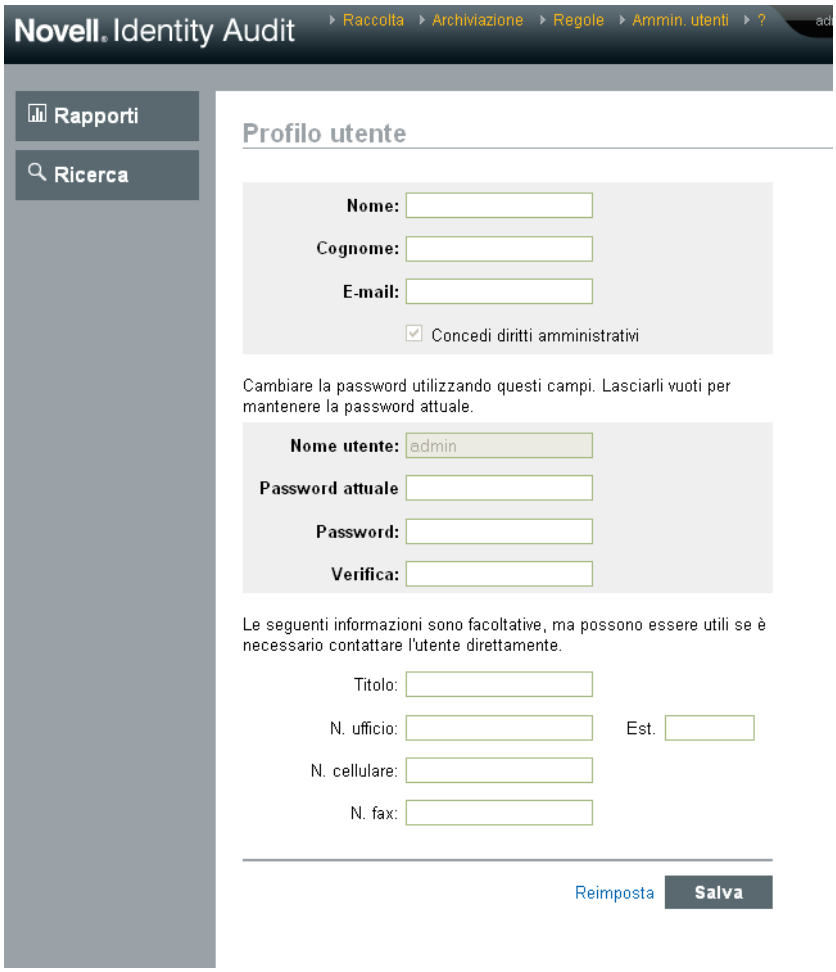
9.2 Modifica dei dettagli di un utente

Gli amministratori possono modificare le informazioni relative a tutti gli utenti presenti nel sistema. Qualsiasi utente può anche modificare tutti i campi del proprio profilo a eccezione del nome utente e dello stato dell'amministratore. Gli utenti possono anche modificare le password.

- Sezione 9.2.1, “Modifica del proprio profilo”, a pagina 64
- Sezione 9.2.2, “Modifica della password”, a pagina 65
- Sezione 9.2.3, “Modifica del profilo di un altro utente (solo per amministratori)”, a pagina 65
- Sezione 9.2.4, “Reimpostazione della password di un altro utente (solo per amministratori)”, a pagina 66

9.2.1 Modifica del proprio profilo

1 Fare clic su *profile* nell'angolo superiore destro.



2 Modificare tutti i campi disponibili.

3 Fare clic su *Salva*.

9.2.2 Modifica della password

Gli utenti possono modificare la propria password se conoscono quella corrente. In caso contrario è necessario che sia un amministratore a reimpostare la password.

1 Fare clic su *profile* nell'angolo superiore destro.

2 Immettere la password corrente.

3 Immettere la nuova password.

4 Confermare la nuova password.

5 Fare clic su *Salva*.

9.2.3 Modifica del profilo di un altro utente (solo per amministratori)

1 Eseguire il login a Identity Audit come amministratore.

2 Fare clic su *User Admin* nell'angolo superiore destro della pagina.

3 Fare clic su *Edit* in corrispondenza dell'utente da modificare.

4 Modificare tutti i campi, a eccezione del nome utente.

5 Fare clic su *Salva*.

Le modifiche a *Grant Administrative Rights* avranno effetto al successivo login dell'utente.

9.2.4 Reimpostazione della password di un altro utente (solo per amministratori)

Per reimpostare la password di un altro utente, vedere la Sezione 9.2.3, “Modifica del profilo di un altro utente (solo per amministratori)”, a pagina 65.

9.3 Eliminazione di un utente

Gli amministrazioni possono eliminare qualsiasi utente dal sistema.

1 Eseguire il login a Identity Audit come amministratore.

2 Fare clic su *User Admin* nell'angolo superiore destro della pagina.

3 Fare clic su *Edit* in corrispondenza dell'utente da eliminare.

4 Fare clic su *Delete this user* nell'angolo superiore destro della pagina.

5 Fare clic su *Delete* per confermare.

Truststore

A

L'utilizzo dell'autenticazione chiusa per la connessione tra Identity Audit e le applicazioni Novell da cui raccoglie i dati consente di migliorare la sicurezza dei dati.

A.1 Creazione di un archivio di chiavi

Un archivio di chiavi può essere creato mediante l'eseguibile "keytool" di Java, disponibile con qualsiasi installazione jre. Questo archivio di chiavi contiene una coppia di chiavi pubblica e privata che può essere utilizzata per sostituire il certificato di default disponibile con Identity Audit. Di seguito sono riportate istruzioni di base, ma per ulteriori informazioni su keytool, vedere il sito Web Sun (http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html).

1. Individuare la directory /bin per Java, ad esempio `$JAVA_HOME/bin`.
2. Eseguire il comando seguente:

   ```
   keytool -genkey -alias alias -keystore .keystore
   ```

3. Immettere una password per l'archivio di chiavi. Questa password verrà utilizzata durante l'importazione del truststore.
4. Immettere le seguenti informazioni: nome e cognome.
   - Nome e cognome
   - Unità organizzativa
   - Organizzazione
   - Città o località
   - Stato o provincia
   - Sigla della provincia
5. Verificare le informazioni.
6. Premere Invio per utilizzare la stessa password dell'archivio di chiavi.

   Un file .keystore viene creato con una chiave privata e una chiave pubblica corrispondente (certificato).