



# **Insight Security**

## OnCommand Insight

NetApp  
October 24, 2024

# Sommario

Insight Security . . . . .	1
Che cos'è lo strumento securityadmin? . . . . .	1
Modalità di esecuzione . . . . .	1
Comandi . . . . .	2
Azioni coordinate . . . . .	4
Esecuzione di Security Admin Tool - riga di comando . . . . .	6
Esecuzione dello strumento di amministrazione della protezione - modalità interattiva . . . . .	10
Gestione della sicurezza sul server Insight . . . . .	20
Gestione della sicurezza sull'unità di acquisizione locale . . . . .	20
Gestione della sicurezza su una RAU . . . . .	21
Gestione della sicurezza nel Data Warehouse . . . . .	21
Modifica delle password utente interne di OnCommand Insight . . . . .	21

# Insight Security

OnCommand Insight fornisce funzionalità che consentono agli ambienti Insight di operare con una maggiore sicurezza. Queste funzioni includono crittografia, hash delle password e la possibilità di modificare le password interne degli utenti e le coppie di chiavi che crittografano e decrittografano le password. È possibile gestire queste funzioni su tutti i server dell'ambiente Insight utilizzando Securityadmin Tool.

## Che cos'è lo strumento securityadmin?

Lo strumento di amministrazione della protezione supporta l'esecuzione di modifiche al contenuto dei vault e l'esecuzione di modifiche coordinate all'installazione di OnCommand Insight.

Gli usi principali dello strumento securityadmin sono **Backup** e **Restore** della configurazione di protezione (ad esempio, vault) e delle password. Ad esempio, è possibile eseguire il backup del vault su un'unità di acquisizione locale e ripristinarlo su un'unità di acquisizione remota, assicurando la coordinazione delle password in tutto l'ambiente. In alternativa, se nell'ambiente sono presenti più server OnCommand Insight, è possibile eseguire un backup del vault dei server e ripristinarlo in altri server per mantenere le stesse password. Questi sono solo due esempi dei modi in cui è possibile utilizzare securityadmin per garantire la coesione negli ambienti.



Si consiglia vivamente di **eseguire il backup del vault** ogni volta che si esegue il backup di un database OnCommand Insight. In caso contrario, si potrebbe perdere l'accesso.

Lo strumento fornisce entrambe le modalità **interactive** e **command line**.

Molte operazioni dello strumento securityadmin modificano il contenuto del vault e apportano modifiche all'installazione, assicurando che il vault e l'installazione rimangano sincronizzati.

Ad esempio,

- Quando si modifica la password di un utente Insight, la voce dell'utente nella tabella SANscreen.users viene aggiornata con il nuovo hash.
- Quando si modifica la password di un utente MySQL, verrà eseguita l'istruzione SQL appropriata per aggiornare la password dell'utente nell'istanza MySQL.

In alcune situazioni, verranno apportate diverse modifiche all'installazione:

- Quando si modifica l'utente dwh MySQL, oltre ad aggiornare la password nel database MySQL, verranno aggiornate anche più voci di registro per ODBC.

Nelle sezioni seguenti il termine "cambiamenti coordinati" viene utilizzato per descrivere tali cambiamenti.

## Modalità di esecuzione

- Funzionamento normale/predefinito - il servizio server SANscreen deve essere in esecuzione

Per la modalità di esecuzione predefinita, lo strumento securityadmin richiede l'esecuzione del servizio **server SANscreen**. Il server viene utilizzato per l'autenticazione e molte modifiche coordinate all'installazione vengono effettuate tramite chiamate al server.

- Funzionamento diretto - il servizio del server SANscreen potrebbe essere in esecuzione o interrotto.

Se eseguito su un'installazione OCI Server o DWH, lo strumento può essere eseguito anche in modalità "diretta". In questa modalità, l'autenticazione e le modifiche coordinate vengono eseguite utilizzando il database. Il servizio Server non viene utilizzato.

Il funzionamento è identico alla modalità normale, con le seguenti eccezioni:

- L'autenticazione è supportata solo per gli utenti non amministratori di dominio. (Utenti con password e ruoli nel database, non LDAP).
- L'operazione "sostituzione delle chiavi" non è supportata.
- La fase di ri-crittografia del ripristino del vault viene ignorata.
- Modalità di ripristino lo strumento può essere eseguito anche quando l'accesso al server e al database non è possibile (ad esempio perché la password principale nel vault non è corretta).

Quando viene eseguito in questa modalità, l'autenticazione non è possibile e, quindi, non può essere eseguita alcuna operazione con una modifica coordinata dell'installazione.

La modalità di recupero può essere utilizzata per:

- determinare quali voci del vault sono errate (utilizzando l'operazione di verifica)
- sostituire la password di root non corretta con il valore corretto. (Questa operazione non modifica la password. L'utente deve inserire la password corrente).

 Se la password di root nel vault non è corretta e la password non è nota e non è presente alcun backup del vault con la password di root corretta, l'installazione non può essere recuperata utilizzando lo strumento securityadmin. L'unico modo per recuperare l'installazione è quello di reimpostare la password dell'istanza MySQL seguendo la procedura documentata all'indirizzo <https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html>. Dopo aver eseguito la procedura di ripristino, utilizzare l'operazione password memorizzata corretta per immettere la nuova password nel vault.

## Comandi

### Comandi senza restrizioni

I comandi senza restrizioni apportano modifiche coordinate all'installazione (ad eccezione degli archivi di trust). I comandi senza restrizioni possono essere eseguiti senza autenticazione dell'utente.

Comando	Descrizione
vault di backup	Creare un file zip contenente il vault. Il percorso relativo ai file del vault corrisponderà al percorso dei vault rispetto alla radice di installazione. <ul style="list-style-type: none"> <li>• wildfly/standalone/configuration/vault/*</li> <li>• acq/conf/vault/*</li> </ul>
controlla-per-chiavi-predefinite	Verificare se le chiavi del vault corrispondono a quelle del vault di default usato nelle istanze precedenti alla versione 7.3.16.

password-memorizzata-corretta	<p>Sostituire una password (errata) memorizzata nel vault con la password corretta nota all'utente.</p> <p>Questo può essere utilizzato quando il vault e l'installazione non sono coerenti. <b>Notare che non modifica la password effettiva nell'installazione.</b></p>
change-trust-store-password	Modificare la password utilizzata per un archivio attendibile e memorizzare la nuova password nel vault. La password corrente dell'archivio di fiducia deve essere "conosciuta".
verify-keystore	<p>controllare se i valori nel vault sono corretti:</p> <ul style="list-style-type: none"> <li>• Per gli utenti OCI, l'hash della password corrisponde al valore nel database</li> <li>• Per gli utenti MySQL, può essere effettuata una connessione al database</li> <li>• per i keystore, è possibile caricare il keystore e leggere le relative chiavi (se presenti)</li> </ul>
tasti elenco	elencare le voci nel vault (senza mostrare il valore memorizzato)

## Comandi limitati

L'autenticazione è necessaria per qualsiasi comando non nascosto che apporta modifiche coordinate all'installazione:

Comando	Descrizione
restore-vault-backup	<p>Sostituisce il vault corrente con il vault contenuto nel file di backup del vault specificato.</p> <p>Esegue tutte le azioni coordinate per aggiornare l'installazione in modo che corrisponda alle password nel vault ripristinato:</p> <ul style="list-style-type: none"> <li>• Aggiornare le password degli utenti di comunicazione OCI</li> <li>• Aggiornare le password utente MySQL, incluso root</li> <li>• per ogni keystore, se la password del keystore è "conosciuta", aggiornare il keystore usando le password del vault ripristinato.</li> </ul> <p>Quando viene eseguito in modalità normale, legge anche ciascun valore crittografato dall'istanza, lo decrittografa utilizzando il servizio di crittografia del vault corrente, lo crittografa nuovamente utilizzando il servizio di crittografia del vault ripristinato e memorizza il valore crittografato nuovamente.</p>
sincronizza con vault	<p>Esegue tutte le azioni coordinate per aggiornare l'installazione in modo che corrisponda alle password utente nel vault ripristinato:</p> <ul style="list-style-type: none"> <li>• Aggiorna le password degli utenti di comunicazione OCI</li> <li>• Aggiorna le password utente MySQL, incluso root</li> </ul>

change-password (cambia password)	Modifica la password nel vault ed esegue le azioni coordinate.
sostituire le chiavi	Creare un nuovo vault vuoto (che avrà chiavi diverse da quelle esistenti). Quindi copiare le voci dal vault corrente al nuovo vault. Quindi legge ciascun valore crittografato dall'istanza, decrittografarlo utilizzando il servizio di crittografia del vault corrente, crittografarlo nuovamente utilizzando il servizio di crittografia del vault ripristinato e memorizzare il valore crittografato nuovamente.

## Comandi nascosti

Lo strumento SA fornisce i seguenti comandi che non richiedono l'autenticazione ma apportano modifiche coordinate all'installazione.

aggiornamento list-keys (server)	Se l'utente non ha eseguito l'autenticazione, eseguire l'autenticazione utilizzando l'account _interno e la password nel vault corrente. Quindi sostituire il vault corrente con il vault nel file di backup ed eseguire le azioni coordinate.
aggiornamento (acquisizione)	Sostituire il vault corrente con il vault nel file di backup ed eseguire le azioni coordinate.

## Azioni coordinate

### Vault dei server

_interno	Aggiorna hash password per l'utente nel database
acquisizione	Aggiorna hash password per l'utente nel database  Se il vault di acquisizione è presente, aggiornare anche la voce nel vault di acquisizione
dwh_internal	Aggiorna hash password per l'utente nel database
cognos_admin	Aggiorna hash password per l'utente nel database  Se DWH e Windows, aggiornare SANscreen/cognos/Analytics/Configuration/SANscreenAP.properties per impostare la proprietà cognos.admin sulla password.
root	Eseguire SQL per aggiornare la password utente nell'istanza MySQL
inventario	Eseguire SQL per aggiornare la password utente nell'istanza MySQL

dwh	<p>Eseguire SQL per aggiornare la password utente nell'istanza MySQL</p> <p>Se DWH e Windows, aggiornare il registro di Windows per impostare le seguenti voci ODBC sulla nuova password:</p> <ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity\PWD</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity_Efficiency\PWD</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Inventory\PWD</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_performance\PWD</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Ports\PWD</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_cloud_cost\PWD</li> </ul>
dwhuser	Eseguire SQL per aggiornare la password utente nell'istanza MySQL
host	Eseguire SQL per aggiornare la password utente nell'istanza MySQL
password_keystore	Riscrivere il keystore con la nuova password - wildfly/standalone/Configuration/server.keystore
truststore_password	Riscrivere il keystore con la nuova password - wildfly/standalone/Configuration/server.trustore
password_chiave	Riscrivere il keystore con la nuova password - wildfly/standalone/Configuration/sso.jks
archivio_cognos	Nessuno

## Vault di acquisizione

acquisizione	Nessuno
truststore_password	Riscrivere il keystore con la nuova password (se esiste) - acq/conf/cert/client.keystore

## Esecuzione di Security Admin Tool - riga di comando

La sintassi per eseguire lo strumento SA in modalità riga di comando è la seguente:

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-options>
```

where

-s	selects server vault
-au	selects acquisition vault
-db	selects direct operation mode

-lu <user>	user for authentication
-lp <password>	password for authentication
<addition-options>	specifies command and command arguments as described below

Note:

- L'opzione "-i" potrebbe non essere presente sulla riga di comando (in quanto questo seleziona la modalità interattiva).
- per le opzioni "-s" e "-au":
  - "-s" non è consentito su una RAU
  - "-au" non è consentito su DWH
  - se nessuno dei due è presente, allora
    - Il vault del server è selezionato su Server, DWH e Dual
    - Il vault di acquisizione viene selezionato su RAU
- Le opzioni -lu e -lp vengono utilizzate per l'autenticazione dell'utente.
  - Se viene specificato <user> e <password> non lo è, all'utente verrà richiesta la password.
  - Se <user> non viene fornito ed è richiesta l'autenticazione, all'utente verranno richiesti sia <user> che <password>.

## Comandi:

Comando	Utilizzo
password-memorizzata-corretta	<pre>securityadmin [-s</pre>
-au] [-db] -pt <key> [<value>]	<p>vault di backup</p> <p>where</p> <p>-pt specifies the command ("put") &lt;key&gt; is the key &lt;value&gt; is the value. If not present, user will be prompted for value</p>
securityadmin [-s	<p>-au] [-db] -b [&lt;backup-dir&gt;]</p> <p>where</p> <p>-b specified command &lt;backup-dir&gt; is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip</p>
vault di backup	<pre>securityadmin [-s</pre>
-au] [-db] -ub <backup-file>	tasti elenco
where	
-ub specified command ("upgrade-backup") <backup-file> The location to write the backup file	

<pre>securityadmin [-s</pre>	<p><b>-au] [-db] -l</b></p> <p>where</p> <p><b>-l</b> specified command</p>
<p>tasti di controllo</p>	<pre>securityadmin [-s</pre>
<p><b>-au] [-db] -ck</b></p> <p>where</p> <p><b>-ck</b> specified command</p> <p>exit code: 1 error 2 default key(s) 3 unique keys</p>	<p><b>verify-keystore (server)</b></p>
<pre>securityadmin [-s] [-db] -v</pre> <p>where</p> <p><b>-v</b></p> <p>specified command</p>	<p><b>eseguire l'upgrade</b></p>
<pre>securityadmin [-s</pre>	<p><b>-au] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -u</b></p> <p>where</p> <p><b>-u</b> specified command</p> <p>For server vault, if <b>-lu</b> is not present, then authentication will be performed for <b>&lt;user&gt;</b> = <b>_internal</b> and <b>&lt;password&gt;</b> = <b>_internal's password</b> from vault. For acquisition vault, if <b>-lu</b> is not present, then no authentication will be attempted</p>

sostituire le chiavi	<pre>securityadmin [-s</pre>
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command	restore-vault-backup
securityadmin [-s	 <pre>-au] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -r &lt;backup-file&gt;</pre> where -r specified command <backup-file> the backup file location
modifica-password (server)	<pre>securityadmin [-s] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -up -un &lt;user&gt; -p [&lt;password&gt;] [-sh]</pre> where  <pre>-up           specified command ("update-password") -un &lt;user&gt;      entry ("user") name to update -p &lt;password&gt; new password. If &lt;password&gt; not supplied, user will be prompted. -sh           for mySQL user, use strong hash</pre>
modifica password per l'utente di acquisizione (acquisizione)	<pre>securityadmin [-au] [-db] [-lu &lt;user&gt;] [-lp &lt;password&gt;] -up -p [&lt;password&gt;]</pre> where  <pre>-up           specified command ("update-password") -p &lt;password&gt; new password. If &lt;password&gt; not supplied, user will be prompted.</pre>

change-password per  
truststore\_password  
(acquisizione)

```
securityadmin [-au] [-db] [-lu <user>] [-lp  
<password>] -utp -p [<password>]
```

where

-utp specified command ("update-truststore-  
password")  
-p <password> new password. If <password> not  
supplied, user will be prompted.

sincronizza con vault  
(server)

```
securityadmin [-s] [-db] [-lu <user>] [-lp <password>]  
-sv <backup-file>
```

where

-sv specified command

## Esecuzione dello strumento di amministrazione della protezione - modalità interattiva

### Interattivo - Menu principale

Per eseguire lo strumento SA in modalità interattiva, immettere il seguente comando:

```
securityadmin -i
```

In un server o in un'installazione doppia, securityadmin richiederà all'utente di selezionare il server o l'unità di acquisizione locale.

Rilevati nodi server e unità di acquisizione. Selezionare il nodo di cui si desidera riconfigurare la protezione:

1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:

In DWH, "Server" viene selezionato automaticamente. Su un'unità AU remota, viene selezionata automaticamente l'opzione "Acquisition Unit" (unità di acquisizione).

## Interactive - Server: Recupero della password di root

In modalità Server, lo strumento securityadmin controlla innanzitutto che la password root memorizzata sia corretta. In caso contrario, viene visualizzata la schermata di ripristino della password principale.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Se si seleziona l'opzione 1, all'utente verrà richiesta la password corretta.

```
Enter password (blank = don't change)
Enter correct password for 'root':
Se viene inserita la password corretta, viene visualizzato quanto segue.
```

```
Password verified. Vault updated
Premendo invio viene visualizzato il menu senza restrizioni del server.
```

Se viene immessa una password errata, viene visualizzato quanto segue

```
Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Premere invio per tornare al menu di ripristino.
```

Se si seleziona l'opzione 2, all'utente verrà richiesto di specificare il nome di un file di backup da cui leggere la password corretta:

```
Enter Backup File Location:
Se la password del backup è corretta, viene visualizzato quanto segue.
```

```
Password verified. Vault updated
Premendo invio viene visualizzato il menu senza restrizioni del server.
```

Se la password nel backup non è corretta, viene visualizzato quanto segue

```
Password verification failed - Access denied for user 'root'@'localhost'  
(using password: YES)  
Premere invio per tornare al menu di ripristino.
```

## Interactive - Server: Password corretta

L'azione "Password corretta" viene utilizzata per modificare la password memorizzata nel vault in modo che corrisponda alla password effettiva richiesta dall'installazione. Questo comando è utile in situazioni in cui è stata apportata una modifica all'installazione da qualcosa di diverso dallo strumento securityadmin. Alcuni esempi sono:

- La password per un utente SQL è stata modificata mediante l'accesso diretto a MySQL.
- Viene sostituito un archivio chiavi o la password di un archivio chiavi viene modificata utilizzando keytool.
- Un database OCI è stato ripristinato e tale database ha password diverse per gli utenti interni

"Correct Password" (Password corretta) richiede innanzitutto all'utente di selezionare la password per memorizzare il valore corretto.

Replace incorrect stored password with correct password. (Does not change the required password)

Select User: (Enter 'b' to go Back)

- 1 - \_internal
- 2 - acquisition
- 3 - cognos\_admin
- 4 - cognos keystore
- 5 - dwh
- 6 - dwh\_internal
- 7 - dwhuser
- 8 - hosts
- 9 - inventory
- 10 - sso keystore
- 11 - server keystore
- 12 - root
- 13 - server truststore
- 14 - AU truststore

Enter your choice:

Dopo aver selezionato la voce da correggere, all'utente viene richiesto come desidera fornire il valore.

- 1 - Enter {user} password
- 2 - Get {user} password from vault backup
- 9 - Exit

Enter your choice:

Se si seleziona l'opzione 1, all'utente verrà richiesta la password corretta.

```
Enter password (blank = don't change)
Enter correct password for '{user}':
Se viene inserita la password corretta, viene visualizzato quanto segue.
```

```
Password verified. Vault updated
Premendo invio si torna al menu senza restrizioni del server.
```

Se viene immessa una password errata, viene visualizzato quanto segue

```
Password verification failed - {additional information}
Vault entry not updated.
```

Premendo invio si torna al menu senza restrizioni del server.

Se si seleziona l'opzione 2, all'utente verrà richiesto di specificare il nome di un file di backup da cui leggere la password corretta:

```
Enter Backup File Location:
Se la password del backup è corretta, viene visualizzato quanto segue.
```

```
Password verified. Vault updated
Premendo invio viene visualizzato il menu senza restrizioni del server.
```

Se la password nel backup non è corretta, viene visualizzato quanto segue

```
Password verification failed - {additional information}
Vault entry not updated.
```

Premendo invio viene visualizzato il menu senza restrizioni del server.

## Interactive - Server: Verifica del contenuto del vault

Verificare che il contenuto del vault verifichi se il vault dispone di chiavi corrispondenti al vault predefinito distribuito con le versioni OCI precedenti e verifichi se ciascun valore nel vault corrisponde all'installazione.

I possibili risultati per ogni chiave sono:

OK	Il valore del vault è corretto
Non selezionato	Impossibile verificare il valore rispetto all'installazione
PESSIMO	Il valore non corrisponde all'installazione

Mancante

Manca una voce prevista.

Encryption keys secure: unique, non-default encryption keys detected

```
cognos_admin: OK
    hosts: OK
dwh_internal: OK
    inventory: OK
        dwhuser: OK
keystore_password: OK
    dwh: OK
truststore_password: OK
    root: OK
    _internal: OK
cognos_internal: Not Checked
key_password: OK
acquisition: OK
cognos_archive: Not Checked
cognos_keystore_password: Missing
```

Press enter to continue

## Interactive - Server: Backup

Backup richiede la directory in cui deve essere memorizzato il file zip di backup. La directory deve già esistere e il nome del file sarà ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:
```

```
Backup Succeeded!    Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

## Interactive - Server: Login

L'azione di accesso viene utilizzata per autenticare un utente e ottenere l'accesso alle operazioni che modificano l'installazione. L'utente deve disporre di un Privileges di amministrazione. Quando viene eseguito con il server, può essere utilizzato qualsiasi utente amministratore; quando viene eseguito in modalità diretta, l'utente deve essere un utente locale piuttosto che un utente LDAP.

Authenticating via server. Enter user and password

UserName: admin

Password:

oppure

Authenticating via database. Enter local user and password.

UserName: admin

Password:

Se la password è corretta e l'utente è un utente amministratore, viene visualizzato il menu limitato.

Se la password non è corretta, viene visualizzato quanto segue:

Authenticating via database. Enter local user and password.

UserName: admin

Password:

Login Failed!

Se l'utente non è un amministratore, viene visualizzato quanto segue:

Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!

## Interactive - Server: Menu limitato

Una volta effettuato l'accesso, lo strumento visualizza il menu limitato.

Logged in as: admin

Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:

## **Interactive - Server: Cambia password**

L'azione "Cambia password" viene utilizzata per modificare una password di installazione in un nuovo valore.

"Cambia password" richiede innanzitutto all'utente di selezionare la password da modificare.

```
Change Password
Select User: (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Dopo aver selezionato la voce da correggere, se l'utente è un utente MySQL, all'utente verrà chiesto se eseguire un hash sicuro per la password

MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but requires all clients use SSL connections

Use strong password hash? (Y/n) : y

Quindi, all'utente viene richiesta la nuova password.

```
New Password for '{user}':  
If the password is empty, the operation is cancelled.  
  
Password is empty - cancelling operation
```

Se viene immessa una password non vuota, all'utente viene richiesto di confermarla.

```
New Password for '{user}':  
  
Confirm New Password for '{user}':  
  
Password successfully updated for 'dwhuser'!
```

Se la modifica non riesce, viene visualizzato l'errore o l'eccezione.

## Interactive - Server: Ripristino

### Interactive - Server (interattivo - Server): Modifica delle chiavi di crittografia

L'azione Modifica chiavi di crittografia sostituirà la chiave di crittografia utilizzata per crittografare le voci del vault e sostituirà la chiave di crittografia utilizzata per il servizio di crittografia del vault. Poiché la chiave del servizio di crittografia viene modificata, i valori crittografati nel database vengono nuovamente crittografati; vengono letti, decrittografati con la chiave corrente, crittografati con la nuova chiave e salvati nuovamente nel database.

Questa azione non è supportata in modalità diretta poiché il server fornisce l'operazione di ricodifica per alcuni contenuti del database.

```
Replace encryption key with new key and update encrypted database values  
  
Confirm (y/N): y  
  
Change Encryption Keys succeeded! Restart 'Server' Service!
```

## Interactive - Server: Installazione fix

L'azione Correggi installazione aggiornerà l'installazione. Tutte le password di installazione che possono essere modificate tramite lo strumento securityadmin, ad eccezione di root, saranno impostate sulle password nel vault.

- Le password degli utenti interni di OCI verranno aggiornate.
- Le password degli utenti MySQL, ad eccezione di root, verranno aggiornate.
- Le password dei keystore verranno aggiornate.

```
Fix installation - update installation passwords to match values in vault
```

```
Confirm: (y/N) : y
```

```
Installation update succeeded! Restart 'Server' Service.
```

L'azione si interrompe al primo aggiornamento non riuscito e visualizza l'errore o l'eccezione.

## Gestione della sicurezza sul server Insight

Il securityadmin Consente di gestire le opzioni di sicurezza sul server Insight. La gestione della sicurezza include la modifica delle password, la generazione di nuove chiavi, il salvataggio e il ripristino delle configurazioni di sicurezza create o il ripristino delle configurazioni alle impostazioni predefinite.

### A proposito di questa attività

Si utilizza securityadmin tool per gestire la sicurezza:

- Finestre - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

Per ulteriori informazioni, consultare la "["Securityadmin"](#)documentazione.

## Gestione della sicurezza sull'unità di acquisizione locale

Il securityadmin Tool consente di gestire le opzioni di sicurezza sull'utente di acquisizione locale (LAU). La gestione della sicurezza include la gestione di chiavi e password, il salvataggio e il ripristino delle configurazioni di sicurezza create o il ripristino delle impostazioni predefinite delle configurazioni.

### Prima di iniziare

Devi avere admin privilegi per eseguire attività di configurazione della sicurezza.

### A proposito di questa attività

Si utilizza securityadmin tool per gestire la sicurezza:

- Finestre - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

Per ulteriori informazioni, vedere le "["Strumento securityadmin"](#)istruzioni.

## Gestione della sicurezza su una RAU

Il securityadmin Tool consente di gestire le opzioni di sicurezza su Raus. Potrebbe essere necessario eseguire il backup o il ripristino di una configurazione del vault, modificare le chiavi di crittografia o aggiornare le password per le unità di acquisizione.

### A proposito di questa attività

Si utilizza securityadmin tool per gestire la sicurezza:

- Finestre - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

Uno scenario per aggiornare la configurazione di protezione per LAU/RAU è l'aggiornamento della password utente di 'acquisizione' quando la password per quell'utente è stata modificata sul server. LAU e tutti i Raus utilizzano la stessa password dell'utente 'acquisizione' del server per comunicare con il server.

L'utente di "acquisizione" esiste solo sul server Insight. RAU o LAU accedono come tale utente quando si connettono al server.

Per ulteriori informazioni, vedere le "[Strumento securityadmin](#)" istruzioni.

## Gestione della sicurezza nel Data Warehouse

Il securityadmin Consente di gestire le opzioni di sicurezza sul server Data Warehouse. La gestione della sicurezza include l'aggiornamento delle password interne per gli utenti interni sul server DWH, la creazione di backup della configurazione di sicurezza o il ripristino delle configurazioni alle impostazioni predefinite.

### A proposito di questa attività

Si utilizza securityadmin tool per gestire la sicurezza:

- Finestre - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

Per ulteriori informazioni, consultare la "[Securityadmin](#)" documentazione.

## Modifica delle password utente interne di OnCommand Insight

Le policy di sicurezza potrebbero richiedere la modifica delle password nell'ambiente OnCommand Insight. Alcune delle password di un server si trovano su un server diverso dell'ambiente, che richiede la modifica della password su entrambi i server. Ad esempio, quando si modifica la password utente "Inventory" su Insight Server, è necessario corrispondere alla password utente "Inventory" sul connettore del server Data Warehouse configurato per Insight Server.

## Prima di iniziare



Prima di modificare le password, è necessario comprendere le dipendenze degli account utente. Il mancato aggiornamento delle password su tutti i server richiesti causerà errori di comunicazione tra i componenti Insight.

## A proposito di questa attività

La seguente tabella elenca le password utente interne per Insight Server e i componenti Insight con password dipendenti che devono corrispondere alla nuova password.

Password di Insight Server	Modifiche richieste
_interno	
acquisizione	LAU, RAU
dwh_internal	Data Warehouse
host	
inventario	Data Warehouse
root	

La seguente tabella elenca le password utente interne per Data Warehouse ed elenca i componenti Insight che hanno password dipendenti che devono corrispondere alla nuova password.

Password Data Warehouse	Modifiche richieste
cognos_admin	
dwh	
dwh_internal (modificato utilizzando l'interfaccia utente di configurazione di Server Connector)	Server Insight
dwhuser	
host	
Inventario (modificato utilizzando l'interfaccia utente di configurazione di Server Connector)	Server Insight
root	

## Modifica delle password nell'interfaccia utente di configurazione della connessione del server DWH

La seguente tabella elenca la password utente per LAU ed elenca i componenti Insight con password dipendenti che devono corrispondere alla nuova password.

LAU password	Modifiche richieste
acquisizione	Insight Server, RAU

## Modifica delle password "inventario" e "dwh\_internal" utilizzando l'interfaccia utente di configurazione della connessione al server

Se è necessario modificare le password "Inventory" o "dwh\_internal" in modo che corrispondano a quelle del server Insight, utilizzare l'interfaccia utente di Data Warehouse.

### Prima di iniziare

Per eseguire questa attività, è necessario essere connessi come amministratore.

### Fasi

1. Accedere al Data Warehouse Portal all'indirizzo <https://hostname/dwh>, Dove hostname è il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Dal riquadro di navigazione a sinistra, fare clic su **connettori**.

Viene visualizzata la schermata **Edit Connector** (Modifica connettore).

**Edit Connector**

ID:	1
Encryption:	Enabled
Name:	Oci-stg06-s12r2.nane.netapp.com
Host:	Oci-stg06-s12r2.nane.netapp.com
Database user name:	inventory
Database password:	*****

**Advanced** ▾

**Save** **Cancel** **Test** **Remove**

3. Immettere una nuova password "Inventory" per il campo **Database password**.
4. Fare clic su **Save** (Salva)
5. Per modificare la password "dwh\_internal", fare clic su **Advanced**.

Viene visualizzata la schermata Edit Connector Advanced (Modifica avanzate connettore).

## Edit Connector

ID: 1

Encryption: Enabled

Name: Oci-stg06-s12r2.nane.netapp.com

Host: Oci-stg06-s12r2.nane.netapp.com

Database user name: inventory

Database password: \*\*\*\*\*

Server user name: dwh\_internal

Server password: \*\*\*\*\*

HTTPS port: 443

TCP port: 3306

**Basic** ▲

Save Cancel Test Remove

6. Inserire la nuova password nel campo **Server password**:

7. Fare clic su Save (Salva)

## Modifica della password dwh mediante lo strumento di amministrazione ODBC

Quando si modifica la password per l'utente dwh sul server Insight, la password deve essere modificata anche sul server Data Warehouse. Utilizzare lo strumento Amministratore origine dati ODBC per modificare la password nel Data Warehouse.

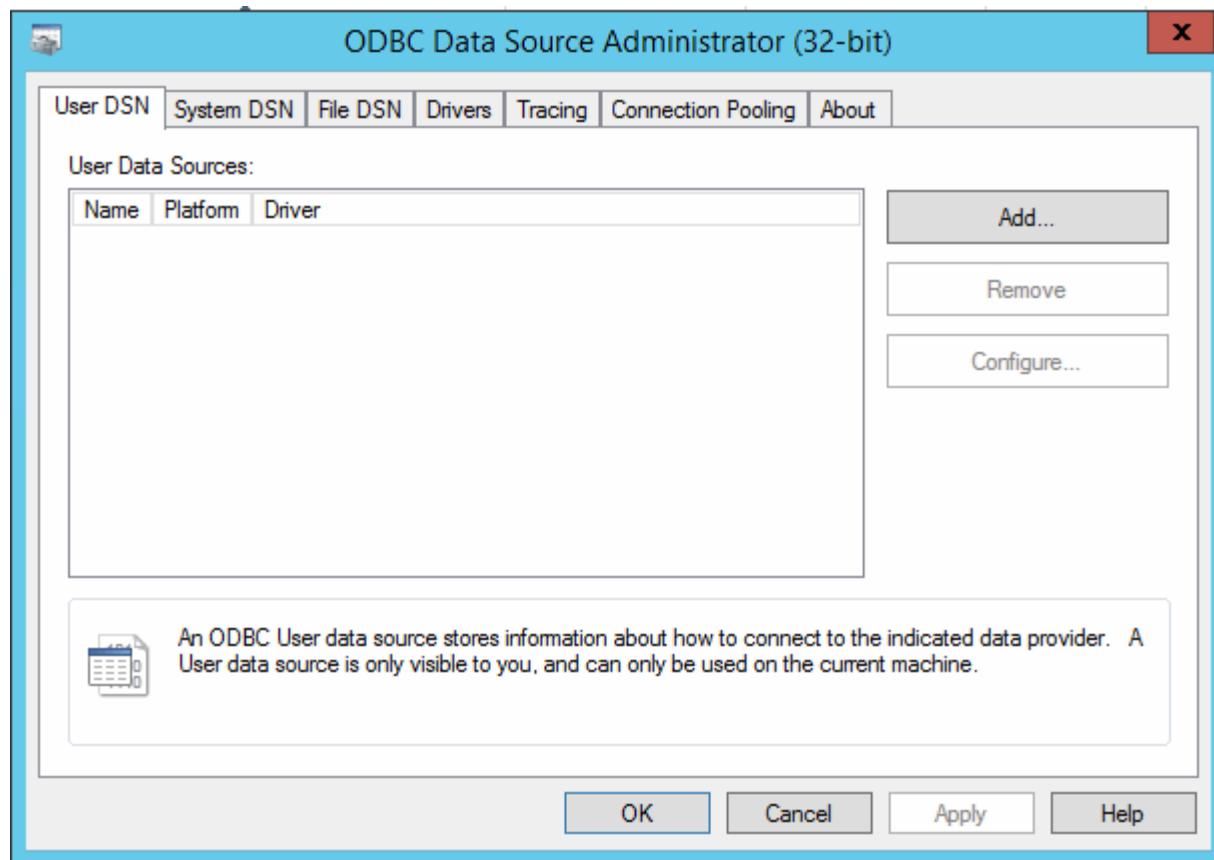
### Prima di iniziare

È necessario eseguire un accesso remoto al server Data Warehouse utilizzando un account con privilegi di amministratore.

### Fasi

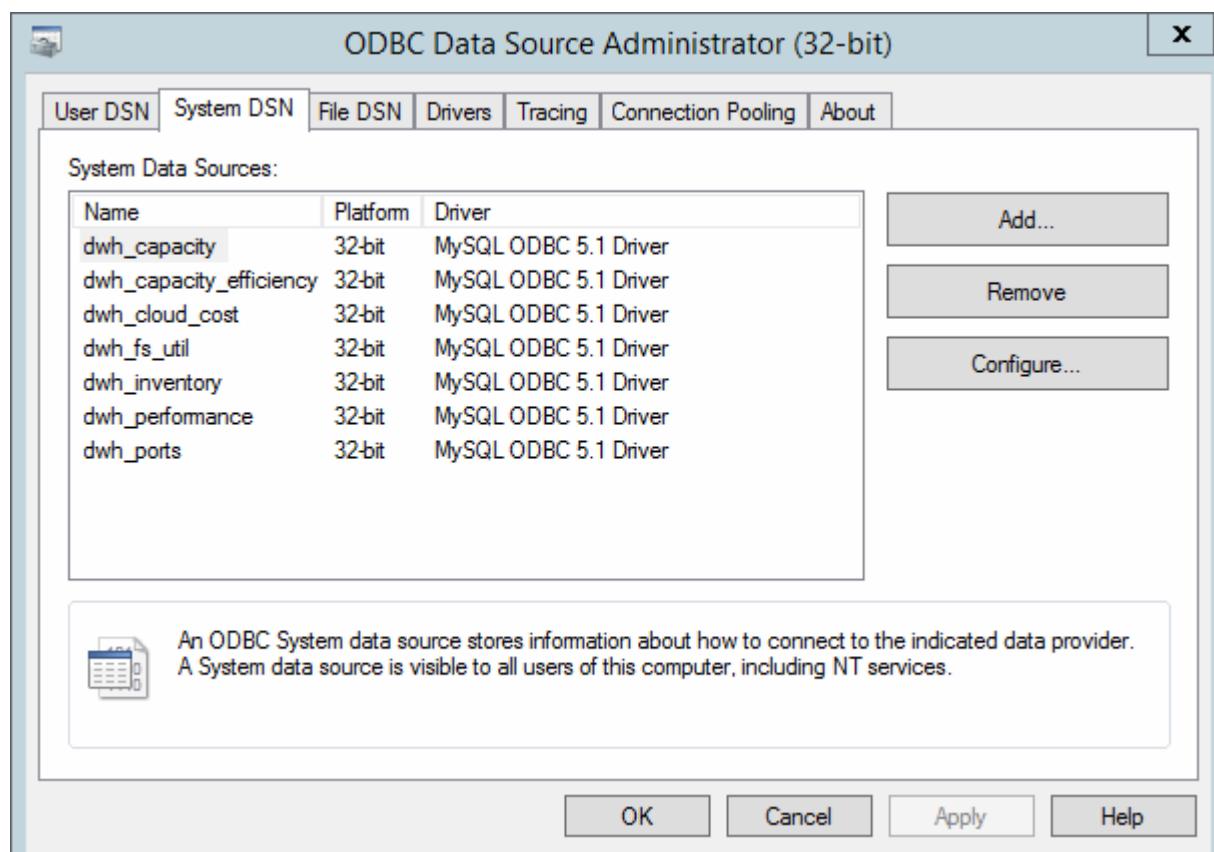
1. Eseguire un login remoto al server che ospita il Data Warehouse.
2. Accedere allo strumento di amministrazione ODBC all'indirizzo C:\Windows\SysWOW64\odbcad32.exe

Viene visualizzata la schermata Amministratore origine dati ODBC.



### 3. Fare clic su **DSN di sistema**

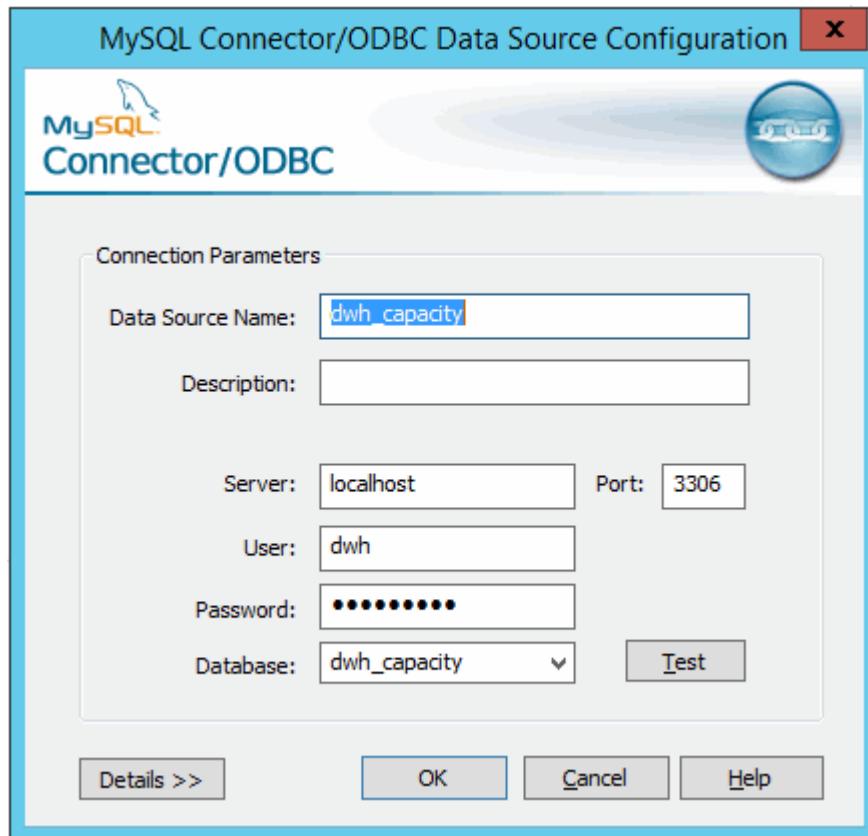
Vengono visualizzate le origini dati di sistema.



4. Selezionare un'origine dati OnCommand Insight dall'elenco.

5. Fare clic su **Configura**

Viene visualizzata la schermata Data Source Configuration (Configurazione origine dati).



6. Inserire la nuova password nel campo **Password**.

## **Informazioni sul copyright**

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

**LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE:** l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## **Informazioni sul marchio commerciale**

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.