



Insight Security

OnCommand Insight

NetApp
April 01, 2024

This PDF was generated from <https://docs.netapp.com/it-it/oncommand-insight/config-admin/managing-security-on-the-insight-server.html> on April 01, 2024. Always check docs.netapp.com for the latest.

Sommario

- Insight Security 1
 - Codifica dei server 1
 - Modifica della password utente di acquisizione 1
 - Considerazioni sull'aggiornamento e l'installazione 1
 - Gestione delle chiavi in un ambiente di service provider complesso 1
 - Gestione della sicurezza sul server Insight 2
 - Gestione della sicurezza sull'unità di acquisizione locale 4
 - Gestione della sicurezza su una RAU 6
 - Gestione della sicurezza nel Data Warehouse 7
 - Modifica delle password utente interne di OnCommand Insight 9

Insight Security

La versione 7.3.1 di OnCommand Insight ha introdotto funzionalità di sicurezza che consentono agli ambienti Insight di funzionare con una maggiore sicurezza. Le funzionalità includono miglioramenti alla crittografia, all'hashing delle password e alla possibilità di modificare le password utente interne e le coppie di chiavi che crittografano e decrittano le password. È possibile gestire queste funzionalità su tutti i server dell'ambiente Insight.

L'installazione predefinita di Insight include una configurazione di sicurezza in cui tutti i siti dell'ambiente condividono le stesse chiavi e le stesse password predefinite. Per proteggere i dati sensibili, NetApp consiglia di modificare le chiavi predefinite e la password utente di acquisizione dopo un'installazione o un aggiornamento.

Le password crittografate dell'origine dati vengono memorizzate nel database di Insight Server. Il server dispone di una chiave pubblica e crittografa le password quando un utente le inserisce in una pagina di configurazione dell'origine dati WebUI. Il server non dispone delle chiavi private necessarie per decrittare le password dell'origine dati memorizzate nel database del server. Solo le unità di acquisizione (LAU, RAU) dispongono della chiave privata dell'origine dati necessaria per decrittare le password dell'origine dati.

Codifica dei server

L'utilizzo delle chiavi predefinite introduce una vulnerabilità a livello di sicurezza nell'ambiente in uso. Per impostazione predefinita, le password dell'origine dati vengono memorizzate crittografate nel database Insight. Vengono crittografati utilizzando una chiave comune a tutte le installazioni Insight. In una configurazione predefinita, un database Insight inviato a NetApp include password che in teoria potrebbero essere decifrate da NetApp.

Modifica della password utente di acquisizione

L'utilizzo della password utente predefinita "Acquisition" (acquisizione) introduce una vulnerabilità di sicurezza nell'ambiente. Tutte le unità di acquisizione utilizzano l'utente "Acquisition" per comunicare con il server. Raus con password predefinite può in teoria connettersi a qualsiasi server Insight utilizzando password predefinite.

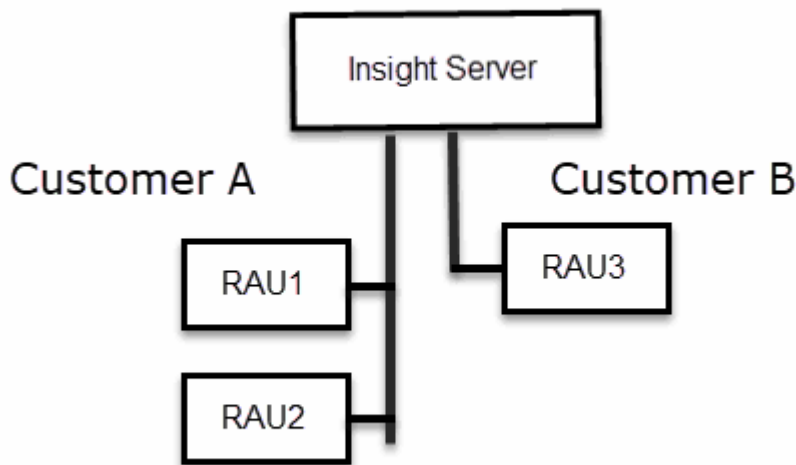
Considerazioni sull'aggiornamento e l'installazione

Se il sistema Insight contiene configurazioni di sicurezza non predefinite (password ridgettate o modificate), è necessario eseguire il backup delle configurazioni di sicurezza. L'installazione di un nuovo software o, in alcuni casi, l'aggiornamento del software ripristina la configurazione di sicurezza predefinita del sistema. Quando il sistema torna alla configurazione predefinita, è necessario ripristinare la configurazione non predefinita per il corretto funzionamento del sistema.

Gestione delle chiavi in un ambiente di service provider complesso

Un service provider può ospitare più clienti OnCommand Insight che raccolgono dati. Le chiavi proteggono i dati dei clienti dall'accesso non autorizzato da parte di più clienti sul server Insight. I dati di ciascun cliente sono protetti dalle coppie di chiavi specifiche.

Questa implementazione di Insight può essere configurata come mostrato nell'illustrazione seguente.



In questa configurazione, è necessario creare singole chiavi per ciascun cliente. Il cliente A richiede chiavi identiche per entrambi i Raus. Il cliente B richiede un singolo set di chiavi.

La procedura da seguire per modificare le chiavi di crittografia per il cliente A:

1. Eseguire un login remoto al server che ospita RAU1.
2. Avviare lo strumento di amministrazione della protezione.
3. Selezionare Change Encryption Key (Cambia chiave di crittografia) per sostituire le chiavi predefinite.
4. Selezionare Backup per creare un file zip di backup della configurazione di sicurezza.
5. Eseguire un login remoto al server che ospita RAU2.
6. Copiare il file zip di backup della configurazione di sicurezza in RAU2.
7. Avviare lo strumento di amministrazione della protezione.
8. Ripristinare il backup di sicurezza da RAU1 al server corrente.

La procedura da seguire per modificare le chiavi di crittografia per il cliente B:

1. Eseguire un login remoto al server che ospita RAU3.
2. Avviare lo strumento di amministrazione della protezione.
3. Selezionare Change Encryption Key (Cambia chiave di crittografia) per sostituire le chiavi predefinite.
4. Selezionare Backup per creare un file zip di backup della configurazione di sicurezza.

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

Fasi

1. Eseguire un accesso remoto al server Insight.
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
 - Finestre - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i
 - Linux - /bin/oci-securityadmin.sh -i

Il sistema richiede le credenziali di accesso.

3. Immettere il nome utente e la password di un account con credenziali "Admin".
4. Selezionare **Server**.

Sono disponibili le seguenti opzioni di configurazione del server:

- **Backup**

Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall'utente o nelle seguenti posizioni predefinite:

- Finestre - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

- **Ripristina**

Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.



Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare la chiave di crittografia del server su un server - creare un backup del vault - ripristinare il backup del vault sul secondo server

- **Cambia chiave di crittografia**

Modificare la chiave di crittografia del server utilizzata per crittografare o decrittare le password utente proxy, le password utente SMTP, le password utente LDAP e così via.



Quando si modificano le chiavi di crittografia, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Aggiorna password**

Modificare la password per gli account interni utilizzati da Insight. Vengono visualizzate le seguenti opzioni:

- _interno
- acquisizione
- cognos_admin
- dwh_internal
- host
- inventario
- root



Alcuni account devono essere sincronizzati quando si modificano le password. Ad esempio, se si modifica la password per l'utente di "acquisizione" sul server, è necessario modificare la password per l'utente di "acquisizione" su LAU, RAU e DWH in modo che corrisponda. Inoltre, quando si modificano le password, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

• Ripristina impostazioni predefinite

Ripristina i valori predefiniti delle chiavi e delle password. I valori predefiniti sono quelli forniti durante l'installazione.

• Esci

Uscire da securityadmin tool.

- Scegliere l'opzione che si desidera modificare e seguire le istruzioni.

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

Fasi

1. Eseguire un accesso remoto al server Insight.
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:

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

Il sistema richiede le credenziali di accesso.

3. Immettere il nome utente e la password di un account con credenziali "Admin".
4. Selezionare **Local Acquisition Unit** (unità di acquisizione locale) per riconfigurare la configurazione di sicurezza dell'unità di acquisizione locale.

Vengono visualizzate le seguenti opzioni:

- **Backup**

Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall'utente o nelle seguenti posizioni predefinite:

- Finestre - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

- **Ripristina**

Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.



Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare le chiavi di crittografia sul LAU - creare un backup del vault - ripristinare il backup del vault su ciascuno dei Raus

- **Modifica delle chiavi di crittografia**

Modificare le chiavi di crittografia AU utilizzate per crittografare o decrittare le password del dispositivo.



Quando si modificano le chiavi di crittografia, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Aggiorna password**

Modificare la password per l'account utente di 'acquisizione'.



Alcuni account devono essere sincronizzati quando si modificano le password. Ad esempio, se si modifica la password per l'utente di "acquisizione" sul server, è necessario modificare la password per l'utente di "acquisizione" su LAU, RAU e DWH in modo che corrisponda. Inoltre, quando si modificano le password, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Ripristina impostazioni predefinite**

Ripristina la password utente di acquisizione e le chiavi di crittografia dell'utente di acquisizione sui valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

- **Esci**

Uscire da `securityadmin tool`.

5. Scegliere l'opzione che si desidera configurare e seguire le 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 l'aggiornamento della configurazione di sicurezza per LAU, RAU, è quello di aggiornare la password utente di 'acquisizione' quando la password per quell'utente è stata modificata sul server. Tutti i sistemi Raus e LAU utilizzano la stessa password dell'utente di '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 gestire le opzioni di sicurezza su una RAU, attenersi alla procedura riportata di seguito:

Fasi

1. Eseguire un accesso remoto al server che esegue RAU
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
 - Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
 - Linux - `/bin/oci-securityadmin.sh -i`

Il sistema richiede le credenziali di accesso.

3. Immettere il nome utente e la password di un account con credenziali "Admin".

Il sistema visualizza il menu della RAU.

- **Backup**

Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall'utente o nelle seguenti posizioni predefinite:

- Finestre - `C:\Program Files\SANscreen\backup\vault`
- Linux - `/var/log/netapp/oci/backup/vault`

- **Ripristina**

Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.



Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare le chiavi di crittografia su un server - creare un backup del vault - ripristinare il backup del vault sul secondo server

- **Modifica delle chiavi di crittografia**

Modificare le chiavi di crittografia RAU utilizzate per crittografare o decrittare le password del dispositivo.



Quando si modificano le chiavi di crittografia, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Aggiorna password**

Modificare la password per l'account utente di 'acquisizione'.



Alcuni account devono essere sincronizzati quando si modificano le password. Ad esempio, se si modifica la password per l'utente di "acquisizione" sul server, è necessario modificare la password per l'utente di "acquisizione" su LAU, RAU e DWH in modo che corrisponda. Inoltre, quando si modificano le password, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Ripristina impostazioni predefinite**

Ripristina le chiavi di crittografia e le password ai valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

- **Esci**

Uscire da securityadmin tool.

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

Fasi

1. Eseguire un login remoto al server Data Warehouse.
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:

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

Il sistema richiede le credenziali di accesso.

3. Immettere il nome utente e la password di un account con credenziali "Admin".

Il sistema visualizza il menu Security admin per Data Warehouse:

- **Backup**

Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall'utente o nella posizione predefinita:

- Finestre - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

- **Ripristina**

Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.



Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare le chiavi di crittografia su un server - creare un backup del vault - ripristinare il backup del vault sul secondo server

+

- **Modificare le chiavi di crittografia**

Modificare la chiave di crittografia DWH utilizzata per crittografare o decrittare password come le password del connettore e le password SMTP.

- **Aggiorna password**

Modificare la password per un account utente specifico.

- _interno
- acquisizione
- cognos_admin
- dwh
- dwh_internal
- dwhuser

- host
- inventario
- root



Quando si modificano le password di dwhuser, host, inventario o root, è possibile utilizzare l'hashing delle password SHA-256. Questa opzione richiede che tutti i client che accedono agli account utilizzino connessioni SSL.

+

- **Ripristina impostazioni predefinite**

Ripristina le chiavi di crittografia e le password ai valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

- **Esci**

Uscire da `securityadmin` tool.

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](#) ▼

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.

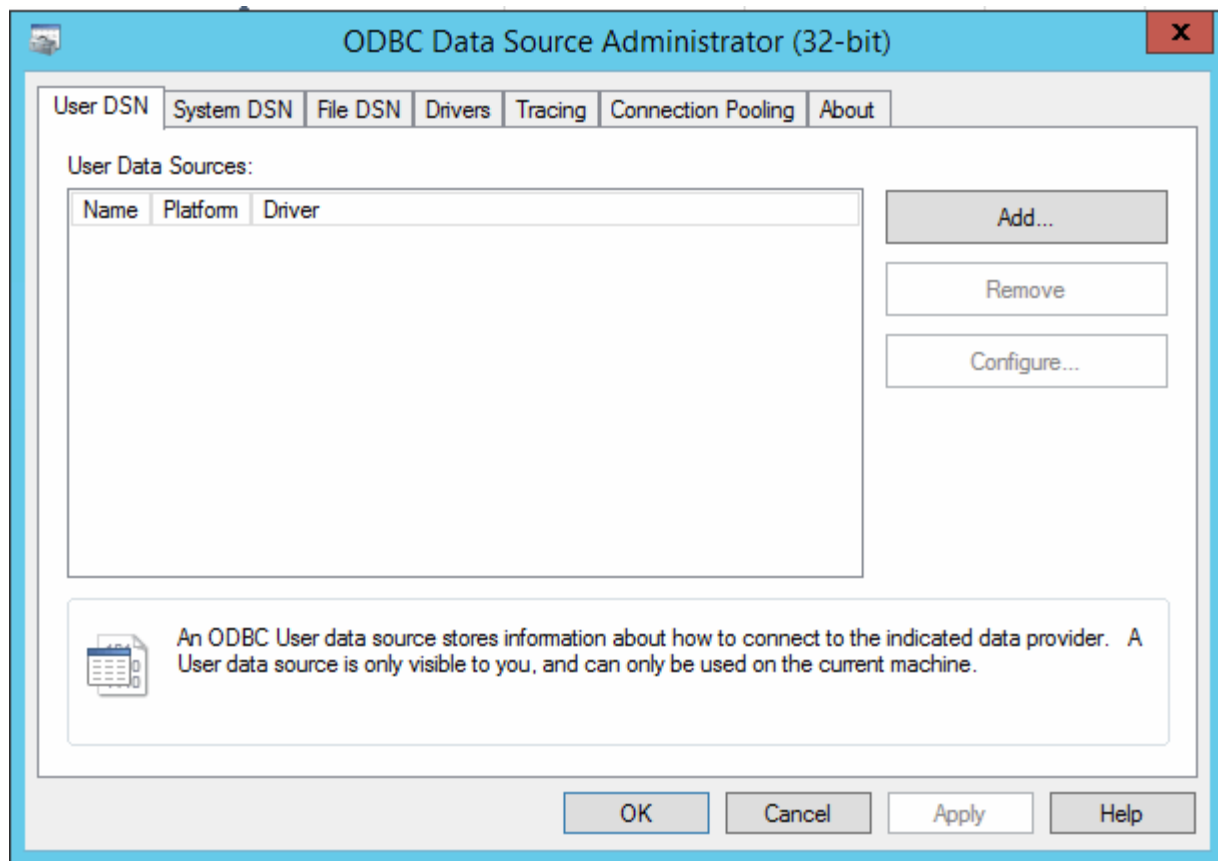
Prima di iniziare

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

Fasi

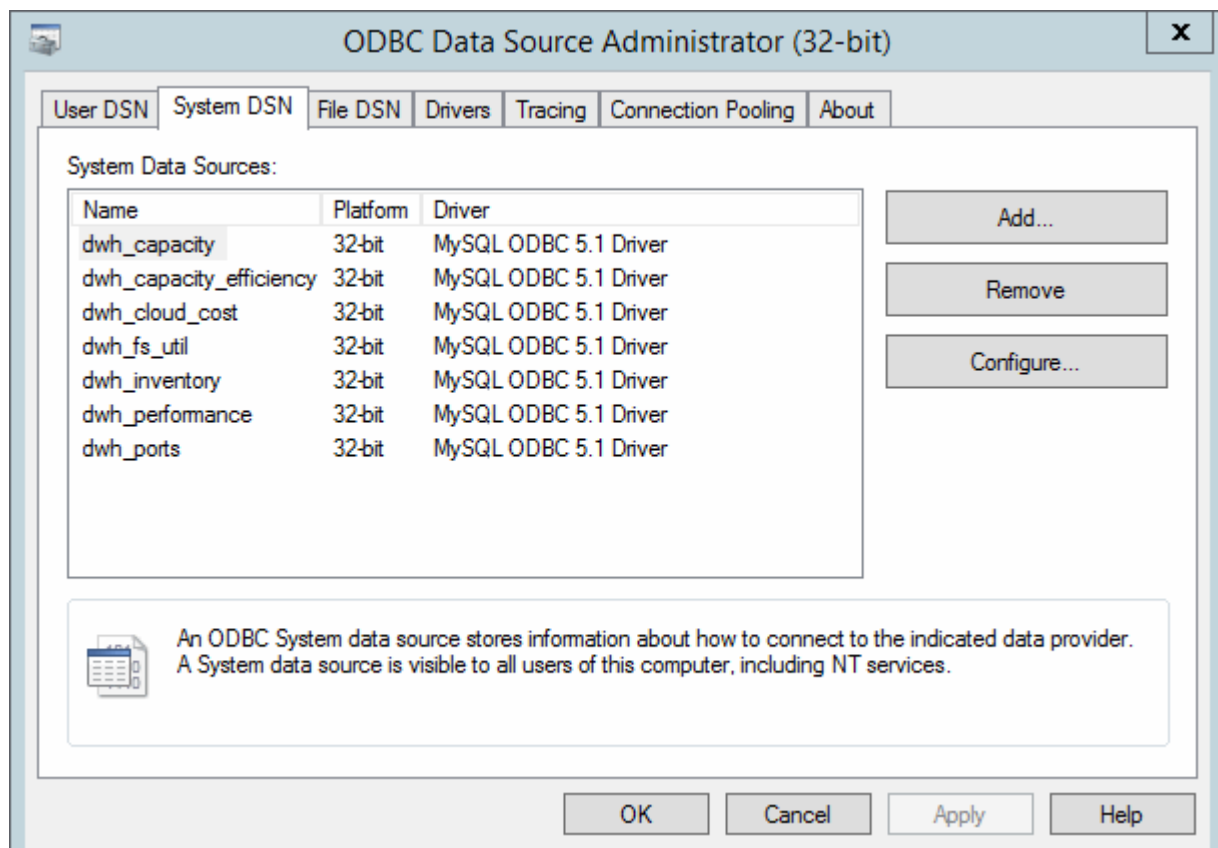
1. Eseguire un login remoto al server che ospita il Data Warehouse.
2. Accedere allo strumento di amministrazione ODBC all'indirizzo `C:\Windows\SysWOW64\odbcad32.exe`

Viene visualizzata la schermata Amministratore origine dati ODBC.



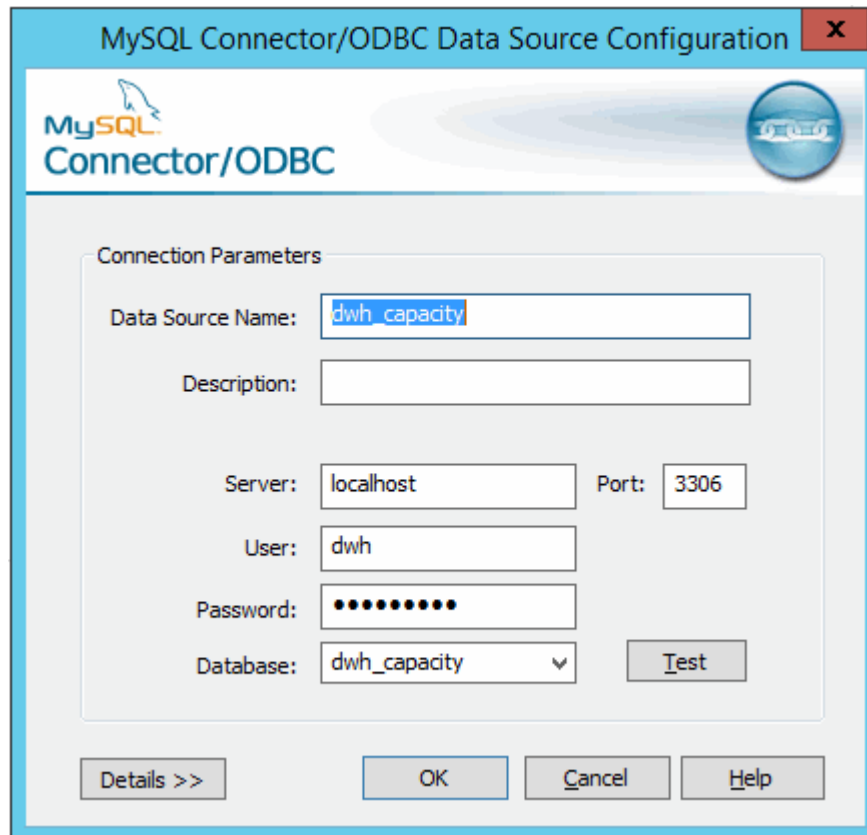
3. Fare clic su **DSN di sistema**

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).



The screenshot shows the 'MySQL Connector/ODBC Data Source Configuration' dialog box. The title bar is blue with the text 'MySQL Connector/ODBC Data Source Configuration' and a red close button. The dialog has a light blue header with the MySQL logo and 'Connector/ODBC' text. Below the header is a 'Connection Parameters' section with a light gray background. It contains the following fields: 'Data Source Name' with the value 'dwh_capacity', 'Description' (empty), 'Server' with 'localhost', 'Port' with '3306', 'User' with 'dwh', 'Password' with masked characters, and 'Database' with a dropdown menu showing 'dwh_capacity'. There is a 'Test' button next to the Database dropdown. At the bottom of the dialog are four buttons: 'Details >>', 'OK', 'Cancel', and 'Help'.

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 COMMERCIALIZZABILITÀ 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.