Insight Security

OnCommand Insight

NetApp
June 10, 2024

This PDF was generated from https://docs.netapp.com/us-en/oncommand-insight/config-admin/managing-security-on-the-insight-server.html on June 10, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Insight Security

The 7.3.1 release of OnCommand Insight introduced security features that allow Insight environments to operate with enhanced security. The features include improvements to encryption, password hashing, and the ability to change internal user passwords and key pairs that encrypt and decrypt passwords. You can manage these features on all servers in the Insight environment.

The default installation of Insight includes a security configuration where all sites in your environment share the same keys and the same default passwords. To protect sensitive data, NetApp recommends you change the default keys and the Acquisition user password after an installation or upgrade.

Data source encrypted passwords are stored in the Insight Server database. The Server has a public key and encrypts passwords when a user enters them in a WebUI data source configuration page. The Server does not have the private keys required to decrypt the data source passwords stored in the Server database. Only Acquisition Units (LAU, RAU) have the data source private key required to decrypt data source passwords.

Rekeying servers

Using default keys introduces security vulnerability in your environment. By default, data source passwords are stored encrypted in the Insight database. They are encrypted using a key that is common to all Insight installations. In a default configuration, an Insight database sent to NetApp includes passwords that could theoretically be decrypted by NetApp.

Changing the Acquisition user password

Using the default 'Acquisition' user password introduces security vulnerability into your environment. All Acquisition Units use the “Acquisition” user to communicate with the Server. RAUs with default passwords can theoretically connect to any Insight server using default passwords.

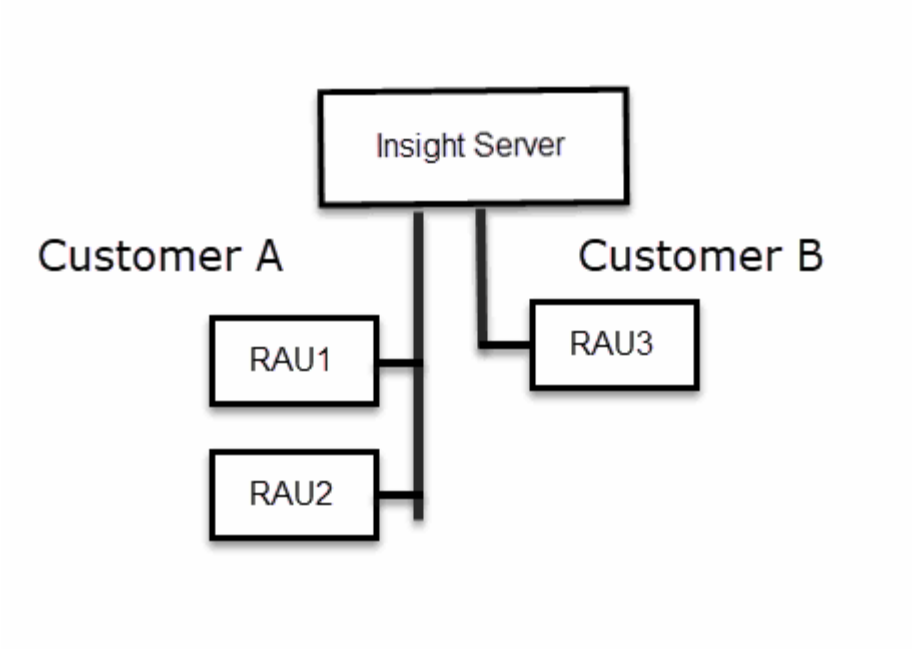
Upgrade and installation considerations

When your Insight system contains non-default security configurations (you have rekeyed or changed passwords), you must back up your security configurations. Installing new software, or in some cases upgrading software, reverts your system to a default security configuration. When your system reverts to the default configuration, you must restore the non-default configuration in order for the system to operate correctly.

Managing keys in a complex service provider environment

A service provider can host multiple OnCommand Insight customers collecting data. The keys protect customer data from unauthorized access by multiple customers on the Insight server. Each customer’s data is protected by their specific key pairs.

This implementation of Insight could be configured as shown in the following illustration.



You need to create individual keys for each customer in this configuration. Customer A requires identical keys for both RAUs. Customer B requires a single set of keys.

The steps you would take to change encryption keys for Customer A:

1. Perform a remote login to the server hosting RAU1.
2. Start the security admin tool.
3. Select Change Encryption Key to replace the default keys.
4. Select Backup to create a backup zip file of the security configuration.
5. Perform a remote login to the server hosting RAU2.
6. Copy the backup zip file of the security configuration to RAU2.
7. Start the security admin tool.
8. Restore the security backup from RAU1 to the current server.

The steps you would take to change encryption keys for Customer B:

1. Perform a remote login to the server hosting RAU3.
2. Start the security admin tool.
3. Select Change Encryption Key to replace the default keys.
4. Select Backup to create a backup zip file of the security configuration.

Managing security on the Insight server

The `securityadmin` tool allows you to manage security options on the Insight server. Security management includes changing passwords, generating new keys, saving and restoring security configurations you create, or restoring configurations to the default settings.

About this task

You use the `securityadmin` tool to manage security:

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

Steps

1. Perform a remote login to the Insight server.
2. Start the security admin tool in interactive mode:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     The system requests login credentials.
3. Enter the user name and password for an account with “Admin” credentials.
4. Select **Server**.

   The following server configuration options are available:

   - **Backup**

     Creates a backup zip file of the vault containing all passwords and keys and places the file in a location specified by the user, or in the following default locations:

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

     Restores the zip backup of the vault that was created. Once restored, all passwords and keys are reverted to values existing at the time of the backup creation.

     Restore can be used to synchronize passwords and keys on multiple servers, for example: - Change the server encryption key on one server - Create a backup of the vault - Restore the vault backup to the second server
   - **Change Encryption Key**

     Change the server encryption key that is used to encrypt or decrypt proxy user passwords, SMTP user passwords, LDAP user passwords, and so on.

     When you change encryption keys, you should backup your new security configuration so that you can restore it after an upgrade or installation.
   - **Update Password**

     Change password for the internal accounts that are used by Insight. The following options are displayed:

- _internal
- acquisition
- cognos_admin
- dwh_internal
- hosts
- inventory
- root

> Some accounts need to be synchronized when passwords are changed. For example, if you change the password for the 'acquisition' user on the server, you need to change the password for the 'acquisition' user on the LAU, RAU, and DWH to match. Also, when you change passwords, you should backup your new security configuration so that you can restore it after an upgrade or installation.

- **Reset to Defaults**

  Resets keys and passwords to default values. Default values are those provided during installation.

- **Exit**

  Exit the `securityadmin` tool.

1. Chose the option you want to change and follow the prompts.

Managing security on the local acquisition unit

The `securityadmin` tool allows you to manage security options on the local acquisition user (LAU). Security management includes managing keys and passwords, saving and restoring security configurations you create or restoring configurations to the default settings.

Before you begin

You must have `admin` privileges to perform security configuration tasks.

About this task

You use the `securityadmin` tool to manage security:

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

Steps

1. Perform a remote login to the Insight server.
2. Start the security admin tool in interactive mode:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`

- Linux - `/bin/oci-securityadmin.sh -i`

  The system requests login credentials.

3. Enter the user name and password for an account with “Admin” credentials.
4. Select **Local Acquisition Unit** to reconfigure the Local Acquisition Unit security configuration.

   The following options are displayed:

   - **Backup**

     Creates a backup zip file of the vault containing all passwords and keys and places the file in a location specified by the user, or in the following default locations:

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

   - **Restore**

     Restores the zip backup of the vault that was created. Once restored, all passwords and keys are reverted to values existing at the time of the backup creation.

     Restore can be used to synchronize passwords and keys on multiple servers, for example: - Change encryption keys on the LAU - Create a backup of the vault - Restore the vault backup to each of the RAUs

   - **Change Encryption Keys**

     Change the AU encryption keys used to encrypt or decrypt device passwords.

     When you change encryption keys, you should backup your new security configuration so that you can restore it after an upgrade or installation.

   - **Update Password**

     Change password for 'acquisition' user account.

     Some accounts need to be synchronized when passwords are changed. For example, if you change the password for the 'acquisition' user on the server, you need to change the password for the 'acquisition' user on the LAU, RAU, and DWH to match. Also, when you change passwords, you should backup your new security configuration so that you can restore it after an upgrade or installation.

   - **Reset to Defaults**

     Resets acquisition user password and acquisition user encryption keys to default values, Default values are those provided during installation.

   - **Exit**

     Exit the `securityadmin` tool.

5. Chose the option you want configure and follow the prompts.

Managing security on an RAU

The `securityadmin` tool allows you to manage security options on RAUs. You might need to backup or restore a vault configuration, change encryption keys, or update passwords for the acquisition units.

About this task

You use the `securityadmin` tool to manage security:

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

One scenario for updating the security configuration for the LAU, RAU is to update the 'acquisition' user password when the password for that user has been changed on the server. All of the RAUs, and the LAU use the same password as that of the server 'acquisition' user to communicate with the server.

The 'acquisition' user only exists on the Insight server. The RAU or LAU logs in as that user when they connect to the server.

Use the following steps to manage security options on an RAU:

Steps

1. Perform a remote login to the server running the RAU
2. Start the security admin tool in interactive mode:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     The system requests login credentials.
3. Enter the user name and password for an account with “Admin” credentials.

   The system displays the menu for the RAU.

   - **Backup**

     Creates a backup zip file of the vault containing all passwords and keys and places the file in a location specified by the user, or in the following default locations:

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

     Restores the zip backup of the vault that was created. Once restored, all passwords and keys are reverted to values existing at the time of the backup creation.

Restore can be used to synchronize passwords and keys on multiple servers, for example: - Change encryption keys on one server - Create a backup of the vault - Restore the vault backup to the second server

- **Change Encryption Keys**

  Change the RAU encryption keys used to encrypt or decrypt device passwords.

  When you change encryption keys, you should backup your new security configuration so that you can restore it after an upgrade or installation.

- **Update Password**

  Change password for 'acquisition' user account.

  Some accounts need to be synchronized when passwords are changed. For example, if you change the password for the 'acquisition' user on the server, you need to change the password for the 'acquisition' user on the LAU, RAU, and DWH to match. Also, when you change passwords, you should backup your new security configuration so that you can restore it after an upgrade or installation.

- **Reset to Defaults**

  Resets encryption keys and passwords to default values. Default values are those provided during installation.

- **Exit**

  Exit the `securityadmin` tool.

Managing security on the Data Warehouse

The `securityadmin` tool allows you to manage security options on the Data Warehouse server. Security management includes updating internal passwords for internal users on the DWH server, creating backups of the security configuration, or restoring configurations to the default settings.

About this task

You use the `securityadmin` tool to manage security:

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

Steps

1. Perform a remote login to the Data Warehouse server.
2. Start the security admin tool in interactive mode:

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

  The system requests login credentials.

3. Enter the user name and password for an account with “Admin” credentials.

   The system displays the security admin menu for the Data Warehouse:

   - **Backup**

     Creates a backup zip file of the vault containing all passwords and keys and places the file in a location specified by the user, or in the default location:

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

   - **Restore**

     Restores the zip backup of the vault that was created. Once restored, all passwords and keys are reverted to values existing at the time of the backup creation.

     Restore can be used to synchronize passwords and keys on multiple servers, for example: - Change encryption keys on one server - Create a backup of the vault - Restore the vault backup to the second server

     +

   - **Change encryption keys**

     Change the DWH encryption key used to encrypt or decrypt passwords such as connector passwords and SMPT passwords.

   - **Update Password**

     Change password for a specific user account.

     - _internal
     - acquisition
     - cognos_admin
     - dwh
     - dwh_internal
     - dwhuser
     - hosts
     - inventory
     - root

     When you change the dwhuser, hosts, inventory, or root passwords, you have the option to use SHA-256 password hashing. This options requires that all clients accessing the accounts use SSL connections.

- **Reset to Defaults**

  Resets encryption keys and passwords to default values. Default values are those provided during installation.

- **Exit**

  Exit the `securityadmin` tool.

Changing OnCommand Insight internal user passwords

Security policies might require you to change the passwords in your OnCommand Insight environment. Some of the passwords on one server exist on a different server in the environment, requiring that you change the password on both servers. For example, when you change the “inventory” user password on the Insight Server you must match the “inventory” user password on the Data Warehouse server Connector configured for that Insight Server.

Before you begin

You should understand the dependencies of the user accounts before you change passwords. Failing to update passwords on all required servers will result in communication failures between the Insight components.

About this task

The following table lists the internal user passwords for the Insight Server and lists the Insight components that have dependent passwords that need to match the new password.

Insight Server Passwords	Required changes
_internal	
acquisition	LAU, RAU
dwh_internal	Data Warehouse
hosts	
inventory	Data Warehouse
root	

The following table lists the internal user passwords for the Data Warehouse and lists the Insight components that have dependent passwords that need to match the new password.

Data Warehouse Passwords	Required changes

cognos_admin	
dwh	
dwh_internal (Changed using the Server Connector configuration UI)	Insight server
dwhuser	
hosts	
inventory (Changed using the Server Connector configuration UI)	Insight server
root	

Changing passwords in the DWH Server Connection Configuration UI

The following table lists the user password for the LAU and lists the Insight components that have dependent passwords that need to match the new password.

LAU Passwords	Required changes
acquisition	Insight Server, RAU

Changing the “inventory” and “dwh_internal” passwords using the Server Connection Configuration UI

If you need to change the “inventory” or “dwh_internal” passwords to match those on the Insight server you use the Data Warehouse UI.

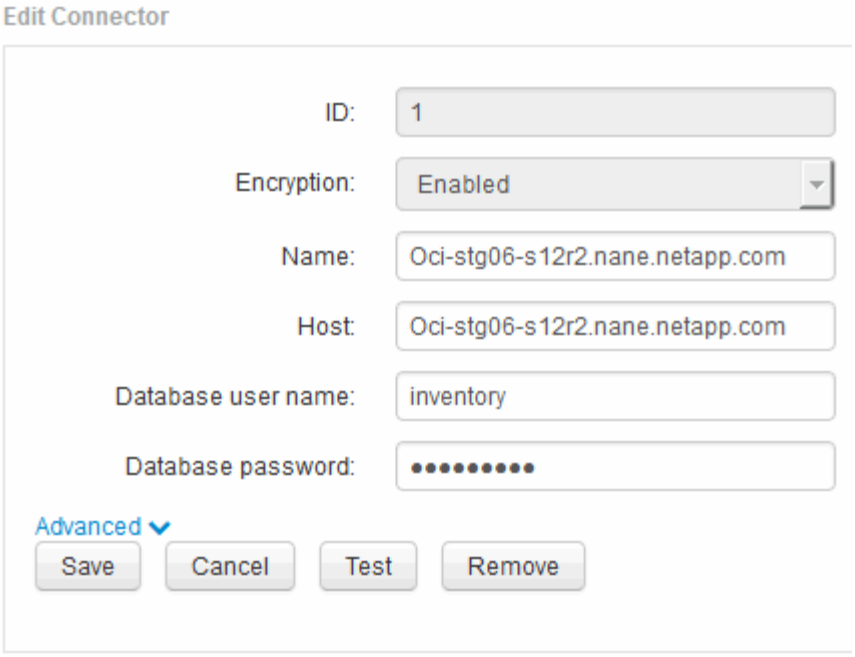
Before you begin

You must be logged in as administrator to perform this task.

Steps

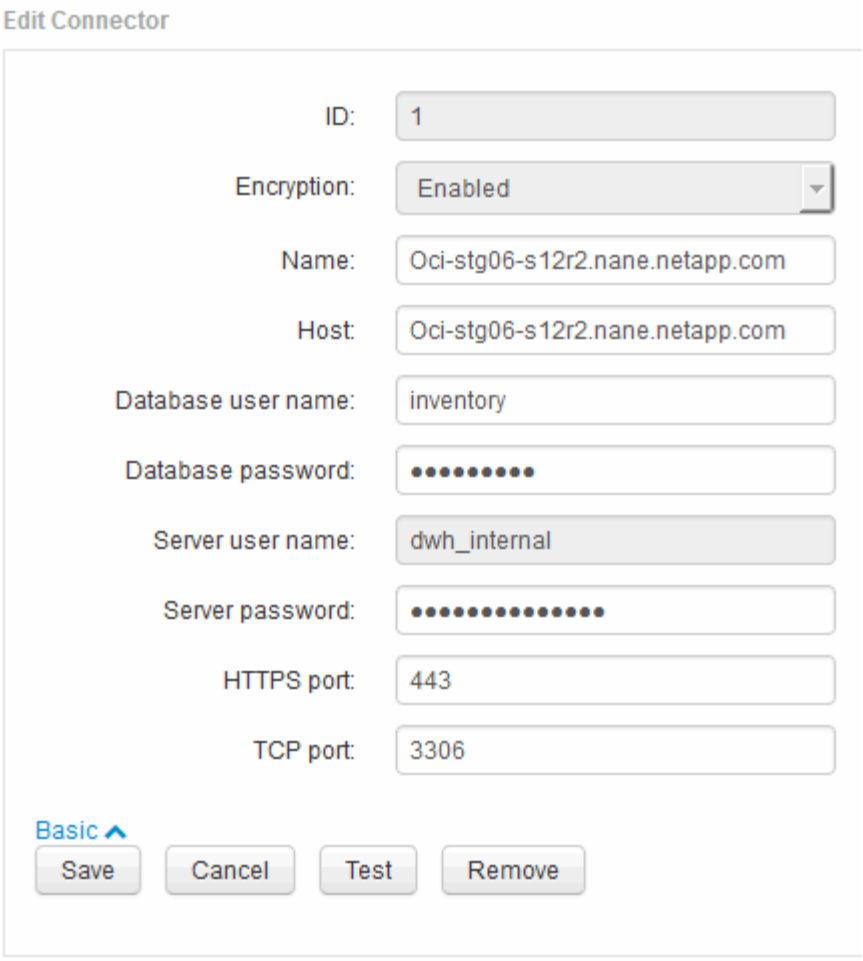
1. Log in to the Data Warehouse Portal at https://hostname/dwh, where hostname is the name of the system where OnCommand Insight Data Warehouse is installed.
2. From the navigation pane on the left, click **Connectors**.

   The **Edit Connector** screen is displayed.



3. Enter a new “inventory” password for the **Database password** field.
4. Click **Save**
5. To change the “dwh_internal” password, click **Advanced.**

   The Edit Connector Advanced screen is displayed.



6. Enter the new password in the **Server password** field:
7. Click save.

Changing the dwh password using the ODBC Administration tool

When you change the password on for the dwh user on the Insight server, the password must also be changed on the Data Warehouse server. You use the ODBC Data Source Administrator tool to change the password on the Data Warehouse.

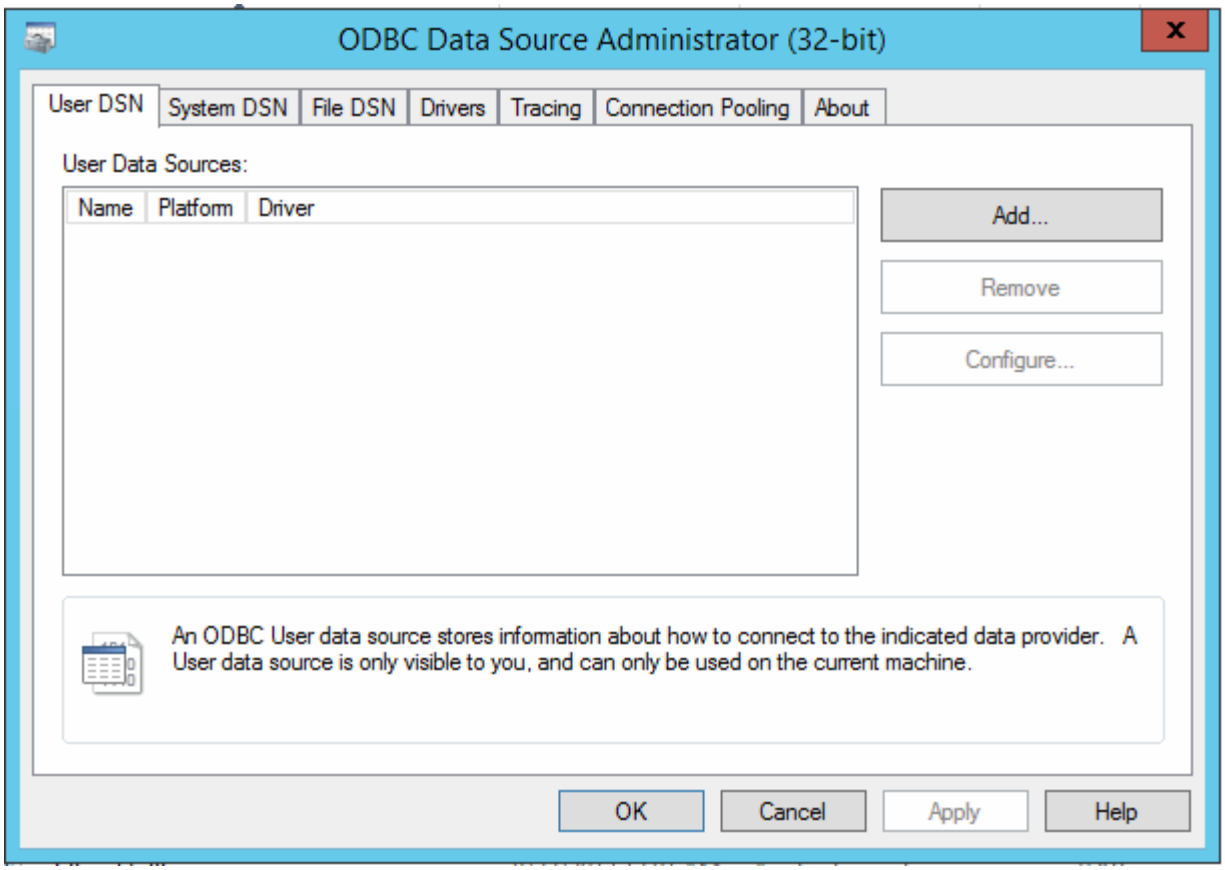
Before you begin

You must perform a remote login to the Data Warehouse server using an account with administrator privileges.

Steps

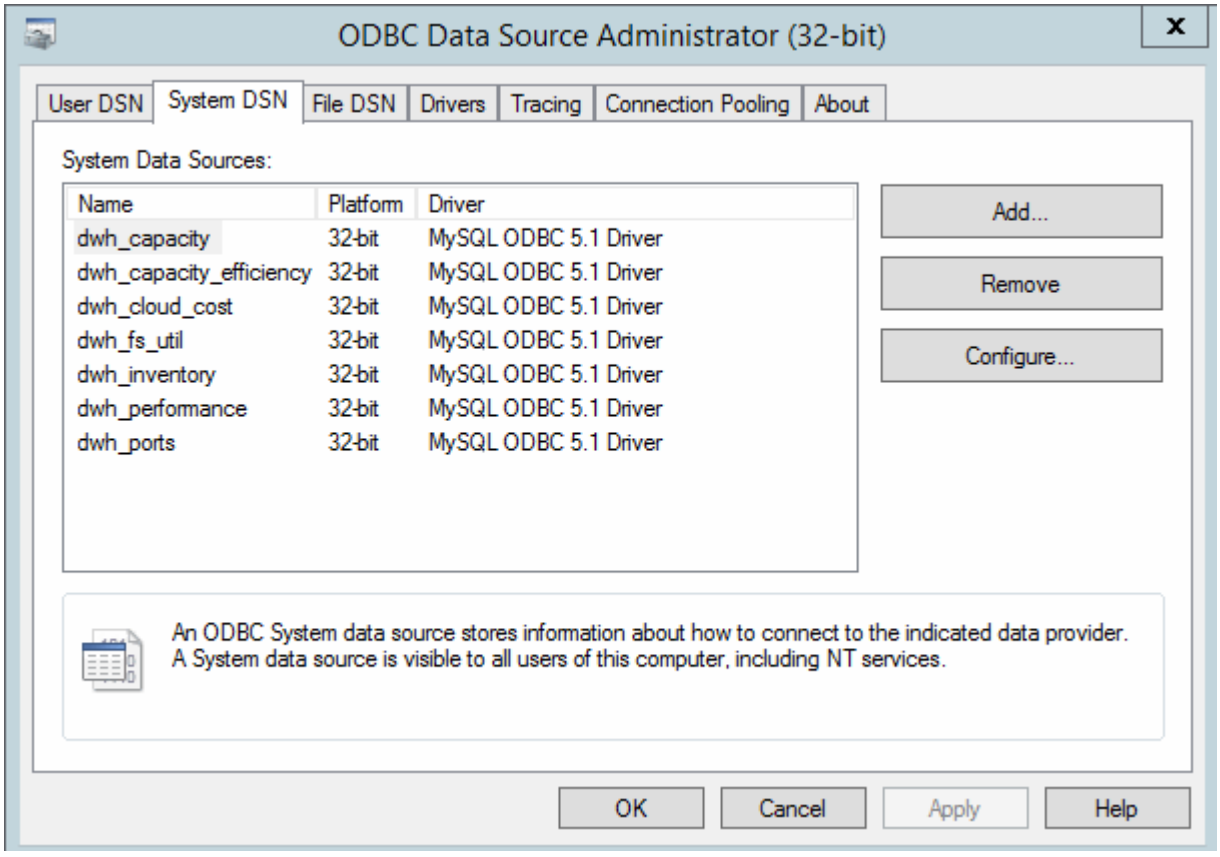
1. Perform a remote login to the server hosting that Data Warehouse.
2. Access the ODBC Administration tool at `C:\Windows\SysWOW64\odbcad32.exe`

   The system displays the ODBC Data Source Administrator screen.



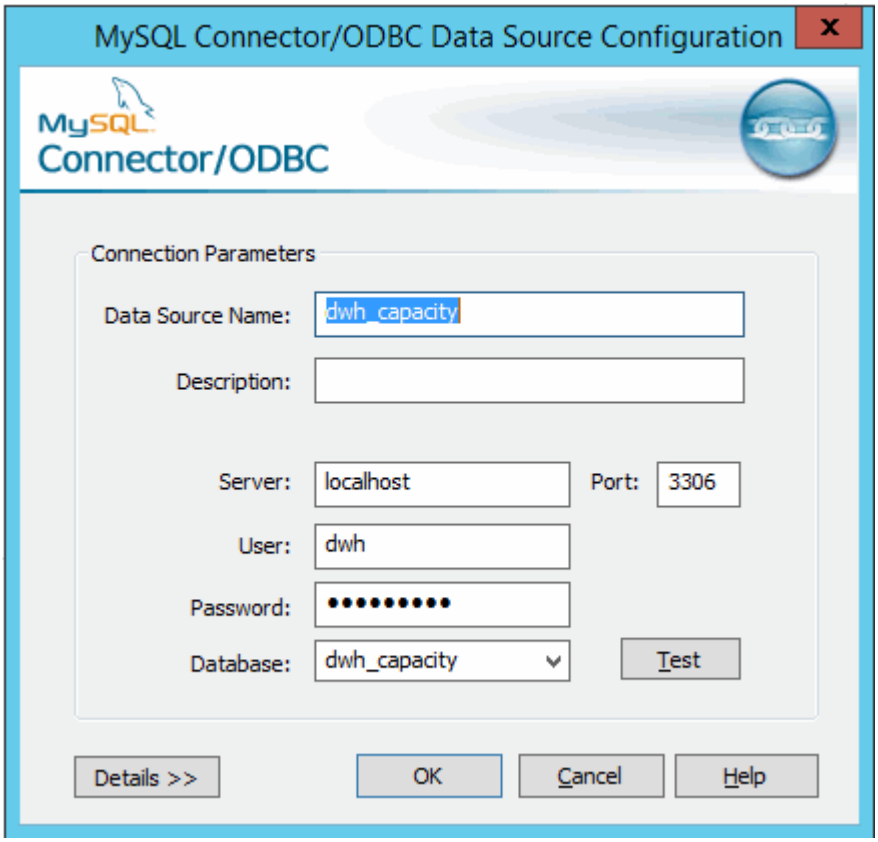
3. Click **System DSN**

   The system data sources are displayed.



4. Select an OnCommand Insight Data Source from the list.
5. Click **Configure**

   The Data Source Configuration screen is displayed.



6. Enter the new password in the **Password** field.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.