



# Insightセキュリティ OnCommand Insight

NetApp  
April 01, 2024

# 目次

Insightセキュリティ .....	1
キーを変更しています .....	1
取得ユーザのパスワードを変更しています .....	1
アップグレードとインストールに関する考慮事項 .....	1
複雑なサービスプロバイダ環境でのキーの管理 .....	1
Insight Serverでセキュリティを管理する .....	2
Local Acquisition Unit上のセキュリティの管理 .....	4
RAUでのセキュリティの管理 .....	6
Data Warehouseでセキュリティを管理する .....	7
OnCommand Insight の内部ユーザのパスワードを変更しています .....	9

# Insightセキュリティ

OnCommand Insight の7.3.1リリースでは、強化されたセキュリティでInsight環境を運用できるようにセキュリティ機能が導入されました。暗号化、パスワードハッシュの強化、内部ユーザパスワードの変更、パスワードの暗号化と復号化を行うキーペアの変更などが含まれます。これらの機能は、Insight環境内のすべてのサーバで管理できます。

Insightのデフォルトのインストールには、環境内のすべてのサイトで同じキーと同じデフォルトパスワードを共有するセキュリティ設定が含まれています。機密データを保護するために、インストールまたはアップグレード後にデフォルトのキーとAcquisitionユーザのパスワードを変更することを推奨します。

データソースで暗号化されたパスワードは、Insight Serverデータベースに保存されます。サーバには公開鍵があり、ユーザがWebUIデータソース設定ページにパスワードを入力すると暗号化されます。サーバには、サーバデータベースに保存されているデータソースパスワードの復号化に必要な秘密鍵がありません。データソースのパスワードの復号化に必要なデータソースの秘密鍵があるのは、Acquisition Unit (LAU、RAU) だけです。

## キーを変更しています

デフォルトキーを使用すると、環境にセキュリティの脆弱性が発生します。デフォルトでは、データソースのパスワードはInsightデータベースに暗号化されて保存されます。すべてのInsight環境に共通のキーを使用して暗号化されます。デフォルトの設定では、ネットアップに送信されるInsightデータベースには、理論的にはネットアップが復号化できるパスワードが含まれています。

## 取得ユーザのパスワードを変更しています

デフォルトの「Acquisition」ユーザパスワードを使用すると、環境にセキュリティの脆弱性がもたらされます。すべてのAcquisition Unitが「Acquisition」ユーザを使用してサーバと通信します。デフォルトのパスワードを使用するRAUは、理論的にはデフォルトのパスワードを使用して任意のInsightサーバに接続できます。

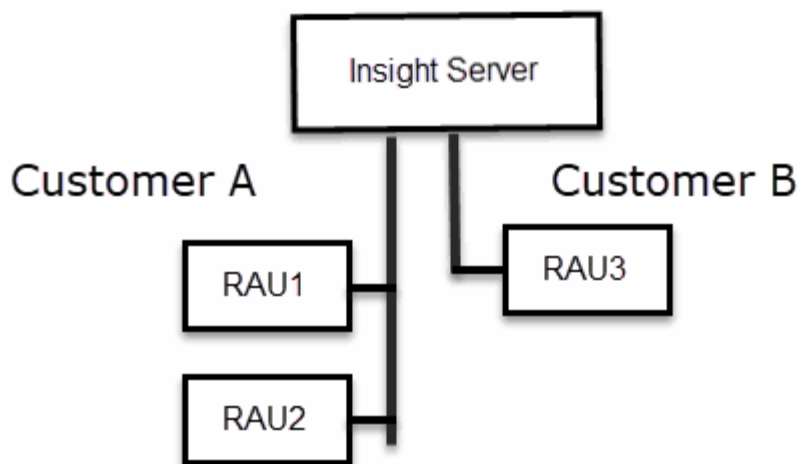
## アップグレードとインストールに関する考慮事項

Insightシステムにデフォルト以外のセキュリティ設定が含まれている場合（パスワードのキーを変更または変更した場合は、セキュリティ設定をバックアップする必要があります。新しいソフトウェアをインストールするか、ソフトウェアをアップグレードする場合によっては、システムをデフォルトのセキュリティ設定に戻します。システムがデフォルトの設定に戻ったら、システムを正常に動作させるために、デフォルト以外の設定をリストアする必要があります。

## 複雑なサービスプロバイダ環境でのキーの管理

サービスプロバイダは、データを収集する複数のOnCommand Insight 顧客をホストできます。これらのキーは、Insight Server上の複数のお客様による不正アクセスからお客様のデータを保護します。各お客様のデータは、それぞれのキーペアによって保護されます。

このInsightの実装は、次の図のように設定できます。



この構成では、顧客ごとに個別のキーを作成する必要があります。お客様Aでは、両方のRAUに同一のキーが必要です。顧客Bは単一のキーセットを必要とします。

顧客Aの暗号化キーを変更する手順は次のとおりです。

1. RAU1をホストしているサーバへのリモートログインを実行します。
2. セキュリティ管理ツールを起動します。
3. デフォルトのキーを置き換えるには、[Change Encryption Key]を選択します。
4. [Backup]を選択して、セキュリティ設定のバックアップzipファイルを作成します。
5. RAU2をホストしているサーバへのリモートログインを実行します。
6. セキュリティ設定のバックアップzipファイルをRAU2にコピーします。
7. セキュリティ管理ツールを起動します。
8. RAU1から現在のサーバにセキュリティバックアップをリストアします。

顧客Bの暗号化キーを変更する手順は次のとおりです。

1. RAU3をホストしているサーバへのリモートログインを実行します。
2. セキュリティ管理ツールを起動します。
3. デフォルトのキーを置き換えるには、[Change Encryption Key]を選択します。
4. [Backup]を選択して、セキュリティ設定のバックアップzipファイルを作成します。

## Insight Serverでセキュリティを管理する

。 securityadmin ツールを使用すると、Insight Serverでセキュリティオプションを管理できます。セキュリティの管理には、パスワードの変更、新しいキーの生成、作成したセキュリティ設定の保存とリストア、デフォルト設定への設定のリストアが含まれま

す。

## このタスクについて

を使用します securityadmin セキュリティ管理ツール：

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

## 手順

1. Insight Serverへのリモートログインを実行します。
2. 対話型モードでセキュリティ管理ツールを起動します。

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

ログインクレデンシャルが要求されます。

3. 「Admin」クレデンシャルを持つアカウントのユーザ名とパスワードを入力します。
4. 「\* サーバー \*」を選択します。

次のサーバ設定オプションを使用できます。

- \* バックアップ \*

すべてのパスワードとキーが格納されているバックアップのzipファイルを作成し、そのファイルをユーザが指定した場所、または次のデフォルトの場所に置きます。

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

- \* 復元 \*

作成したバックアップのzipファイルをリストアします。リストアすると、すべてのパスワードとキーがバックアップ作成時の既存の値に戻ります。



リストアを使用すると、複数のサーバのパスワードとキーを同期できます。例：- 1台のサーバでサーバ暗号化キーを変更-ヴォールトのバックアップを作成-ヴォールトバックアップを2台目のサーバにリストアします

- 暗号化キーの変更

プロキシユーザパスワード、SMTPユーザパスワード、LDAPユーザパスワードなどの暗号化または復号化に使用するサーバ暗号化キーを変更します。



暗号化キーを変更する場合は、アップグレードまたはインストール後にリストアできるように、新しいセキュリティ設定をバックアップする必要があります。

## 。 パスワードの更新

Insightで使用する内部アカウントのパスワードを変更します。次のオプションが表示されます。

- `_internal`
- 取得
- `cognos_admin`をクリックします
- `dwh_internal`の略
- ホスト
- 在庫
- ルート



一部のアカウントは、パスワードを変更したときに同期する必要があります。たとえば、サーバで「acquisition」ユーザのパスワードを変更した場合は、LAU、RAU、DWHでも「acquisition」ユーザのパスワードを同じパスワードに変更する必要があります。また、パスワードを変更する場合は、アップグレードまたはインストール後に復元できるように、新しいセキュリティ設定をバックアップする必要があります。

## • デフォルトにリセット

キーとパスワードをデフォルト値にリセットします。デフォルト値はインストール時に指定された値です。

## • \* 終了 \*

を終了します `securityadmin` ツール。

a. 変更するオプションを選択し、プロンプトの指示に従います。

# Local Acquisition Unit上のセキュリティの管理

。 `securityadmin` ツールを使用すると、Local Acquisition User (LAU；ローカル収集ユーザ) のセキュリティオプションを管理できます。セキュリティの管理には、キーとパスワードの管理、作成したセキュリティ設定の保存とリストア、またはデフォルト設定への設定のリストアが含まれます。

## 作業を開始する前に

が必要です `admin` セキュリティ設定タスクを実行するための権限。

## このタスクについて

を使用します `securityadmin` セキュリティ管理ツール：

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

## 手順

1. Insight Serverへのリモートログインを実行します。
2. 対話型モードでセキュリティ管理ツールを起動します。
  - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
  - Linux - `/bin/oci-securityadmin.sh -i`

ログインクレデンシャルが要求されます。

3. 「Admin」 クレデンシャルを持つアカウントのユーザ名とパスワードを入力します。
4. Local Acquisition Unit \*を選択して、Local Acquisition Unitのセキュリティ設定を再設定します。

次のオプションが表示されます。

- \* バックアップ \*

すべてのパスワードとキーが格納されているバックアップのzipファイルを作成し、そのファイルをユーザが指定した場所、または次のデフォルトの場所に置きます。

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

- \* 復元 \*

作成したバックアップのzipファイルをリストアします。リストアすると、すべてのパスワードとキーがバックアップ作成時の既存の値に戻ります。



リストアを使用すると、複数のサーバのパスワードとキーを同期できます。例：- LAUで暗号化キーを変更-ヴォールトのバックアップを作成-各RAUにヴォールトバックアップをリストアします

- 暗号化キーの変更

デバイスのパスワードの暗号化または復号化に使用するAU暗号化キーを変更します。



暗号化キーを変更する場合は、アップグレードまたはインストール後にリストアできるように、新しいセキュリティ設定をバックアップする必要があります。

- パスワードの更新

「acquisition」 ユーザアカウントのパスワードを変更します。



一部のアカウントは、パスワードを変更したときに同期する必要があります。たとえば、サーバで「acquisition」ユーザのパスワードを変更した場合は、LAU、RAU、DWHでも「acquisition」ユーザのパスワードを同じパスワードに変更する必要があります。また、パスワードを変更する場合は、アップグレードまたはインストール後に復元できるように、新しいセキュリティ設定をバックアップする必要があります。

- デフォルトにリセット

acquisitionユーザのパスワードとacquisitionユーザの暗号化キーをデフォルト値にリセットします。デフォルト値はインストール時に指定したパスワードと暗号化キーです。

◦ \* 終了 \*

を終了します securityadmin ツール。

5. 設定するオプションを選択し、プロンプトの指示に従います。

## RAUでのセキュリティの管理

◦ securityadmin ツールを使用すると、RAUのセキュリティオプションを管理できます。場合によっては、ヴォールト設定のバックアップやリストア、暗号化キーの変更、Acquisition Unitのパスワードの更新が必要になることがあります。

### このタスクについて

を使用します securityadmin セキュリティ管理ツール：

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

LAU (RAU) のセキュリティ設定を更新する1つのシナリオは、サーバで「acquisition」ユーザのパスワードが変更されたときに「acquisition」ユーザのパスワードを更新することです。すべてのRAUおよびLAUでは、サーバとの通信にサーバ「acquisition」ユーザのパスワードと同じパスワードを使用します。

「acquisition」ユーザが存在するのはInsight Serverだけです。RAUまたはLAUは、サーバに接続するときにそのユーザとしてログインします。

RAUでセキュリティオプションを管理するには、次の手順を実行します。

### 手順

1. RAUを実行しているサーバへのリモートログインを実行します
2. 対話型モードでセキュリティ管理ツールを起動します。

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

ログインクレデンシャルが要求されます。

3. 「Admin」クレデンシャルを持つアカウントのユーザ名とパスワードを入力します。

RAUのメニューが表示されます。

◦ \* バックアップ \*

すべてのパスワードとキーが格納されているバックアップのzipファイルを作成し、そのファイルをユーザが指定した場所、または次のデフォルトの場所に置きます。



- Windows - C:\Program Files\SANscreen\backup\vault

- Linux - /var/log/netapp/oci/backup/vault

- \* 復元 \*

作成したバックアップのzipファイルをリストアします。リストアすると、すべてのパスワードとキーがバックアップ作成時の既存の値に戻ります。



リストアを使用すると、複数のサーバのパスワードとキーを同期できます。例：- 1つのサーバで暗号化キーを変更-ヴォールトのバックアップを作成-ヴォールトバックアップを2つ目のサーバにリストアします

- 暗号化キーの変更

デバイスパスワードの暗号化または復号化に使用するRAU暗号化キーを変更します。



暗号化キーを変更する場合は、アップグレードまたはインストール後にリストアできるように、新しいセキュリティ設定をバックアップする必要があります。

- パスワードの更新

「acquisition」ユーザアカウントのパスワードを変更します。



一部のアカウントは、パスワードを変更したときに同期する必要があります。たとえば、サーバで「acquisition」ユーザのパスワードを変更した場合は、LAU、RAU、DWHでも「acquisition」ユーザのパスワードを同じパスワードに変更する必要があります。また、パスワードを変更する場合は、アップグレードまたはインストール後に復元できるように、新しいセキュリティ設定をバックアップする必要があります。

- デフォルトにリセット

暗号化キーとパスワードをデフォルト値にリセットします。デフォルト値はインストール時に指定された値です。

- \* 終了 \*

を終了します securityadmin ツール。

## Data Warehouseでセキュリティを管理する

◦ securityadmin ツールを使用すると、Data Warehouseサーバのセキュリティオプションを管理できます。セキュリティの管理には、DWHサーバで内部ユーザの内部パスワードを更新したり、セキュリティ設定のバックアップを作成したり、設定をデフォルトの設定にリストアしたりする作業があります。

### このタスクについて

を使用します securityadmin セキュリティ管理ツール：

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

## 手順

1. Data Warehouseサーバへのリモートログインを実行します。

2. 対話型モードでセキュリティ管理ツールを起動します。

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

ログインクレデンシャルが要求されます。

3. 「Admin」 クレデンシャルを持つアカウントのユーザ名とパスワードを入力します。

Data Warehouseのセキュリティ管理メニューが表示されます。

### ◦ \* バックアップ \*

すべてのパスワードとキーが格納されたバックアップのzipファイルを作成し、ユーザが指定した場所、またはデフォルトの場所にファイルを配置します。

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

### ◦ \* 復元 \*

作成したバックアップのzipファイルをリストアします。リストアすると、すべてのパスワードとキーがバックアップ作成時の既存の値に戻ります。



リストアを使用すると、複数のサーバのパスワードとキーを同期できます。例：- 1つのサーバで暗号化キーを変更-ヴォールトのバックアップを作成-ヴォールトバックアップを2つ目のサーバにリストアします

[+]

### ◦ 暗号化キーの変更

コネクタのパスワードやSMTPのパスワードなど、パスワードの暗号化や復号化に使用するDWH暗号化キーを変更します。

### ◦ パスワードの更新

特定のユーザアカウントのパスワードを変更します。

- \_internal
- 取得
- cognos\_adminをクリックします
- DWH

- dwh\_internalの略
- 誰だ
- ホスト
- 在庫
- ルート



dwhuser、hosts、inventory、またはrootのパスワードを変更する場合は、SHA-256パスワードハッシュを使用できます。このオプションでは、アカウントにアクセスするすべてのクライアントがSSL接続を使用する必要があります。

+

- デフォルトにリセット

暗号化キーとパスワードをデフォルト値にリセットします。デフォルト値はインストール時に指定された値です。

- \* 終了 \*

を終了します securityadmin ツール。

## OnCommand Insight の内部ユーザのパスワードを変更しています

セキュリティポリシーによっては、OnCommand Insight 環境でパスワードの変更が必要になる場合があります。1台のサーバのパスワードの一部は、環境内の別のサーバに存在するため、両方のサーバでパスワードを変更する必要があります。たとえば、Insight Serverでユーザのパスワード「inventory」を変更する場合は、そのInsight Server用に設定されたData Warehouse Server Connectorでユーザのパスワード「inventory」と一致している必要があります。

### 作業を開始する前に



パスワードを変更する前に、ユーザアカウントの依存関係を理解しておく必要があります。必要なすべてのサーバでパスワードを更新しないと、Insightコンポーネント間の通信に失敗します。

### このタスクについて

次の表に、Insight Serverの内部ユーザパスワードと、依存するパスワードが新しいパスワードと一致する必要があるInsightコンポーネントを示します。

Insight Serverのパスワード	必要な変更
_internal	

取得	愛称はラオ
dwh_internalの略	Data Warehouse
ホスト	
在庫	Data Warehouse
ルート	

次の表に、Data Warehouseの内部ユーザパスワードと、依存するパスワードが新しいパスワードと一致する必要があるInsightコンポーネントを示します。

Data Warehouseのパスワード	必要な変更
cognos_adminをクリックします	
DWH	
dwh_internal（Server Connectorの設定UIを使用して変更）	Insightサーバ
誰だ	
ホスト	
インベントリ（Server Connector設定UIを使用して変更）	Insightサーバ
ルート	

- DWHサーバ接続設定UIでのパスワードの変更\*

次の表に、LAUのユーザパスワードと、依存するパスワードが新しいパスワードと一致する必要があるInsightコンポーネントを示します。

LAUパスワード	必要な変更
取得	Insight Server、RAU

**Server Connection Configuration UI**を使用して「**inventory**」パスワードと「**dwh\_internal**」パスワードを変更します

「inventory」または「dwh\_internal」のパスワードをInsight Serverと同じパスワードに

変更する必要がある場合は、Data Warehouse UIを使用します。

作業を開始する前に

このタスクを実行するには、管理者としてログインする必要があります。

手順

1. Data Warehouseポータルにログインします <https://hostname/dwhhostname>は、OnCommand Insight Data Warehouseがインストールされているシステムの名前です。
2. 左側のナビゲーションペインで、\*[コネクタ]\*をクリックします。

[Edit Connector]（コネクタの編集）\*画面が表示されます。

#### 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. 「\* Database password \*」フィールドに新しい「inventory」パスワードを入力します。
4. [ 保存（ Save ） ] をクリックします。
5. 「dwh\_internal」パスワードを変更するには、\*[詳細設定]\*をクリックします

[Edit Connector Advanced]画面が表示されます。

## Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="....."/>
Server user name:	<input type="text" value="dwh_internal"/>
Server password:	<input type="password" value="....."/>
HTTPS port:	<input type="text" value="443"/>
TCP port:	<input type="text" value="3306"/>

Basic ^

6. 新しいパスワードを\* Server password \*フィールドに入力します。

7. [保存] をクリックします。

## ODBC Administrationツールを使用したDWHパスワードの変更

Insight ServerでDWHユーザのパスワードをで変更した場合は、Data Warehouseサーバでもパスワードを変更する必要があります。ODBC Data Source Administratorツールを使用して、Data Warehouseのパスワードを変更します。

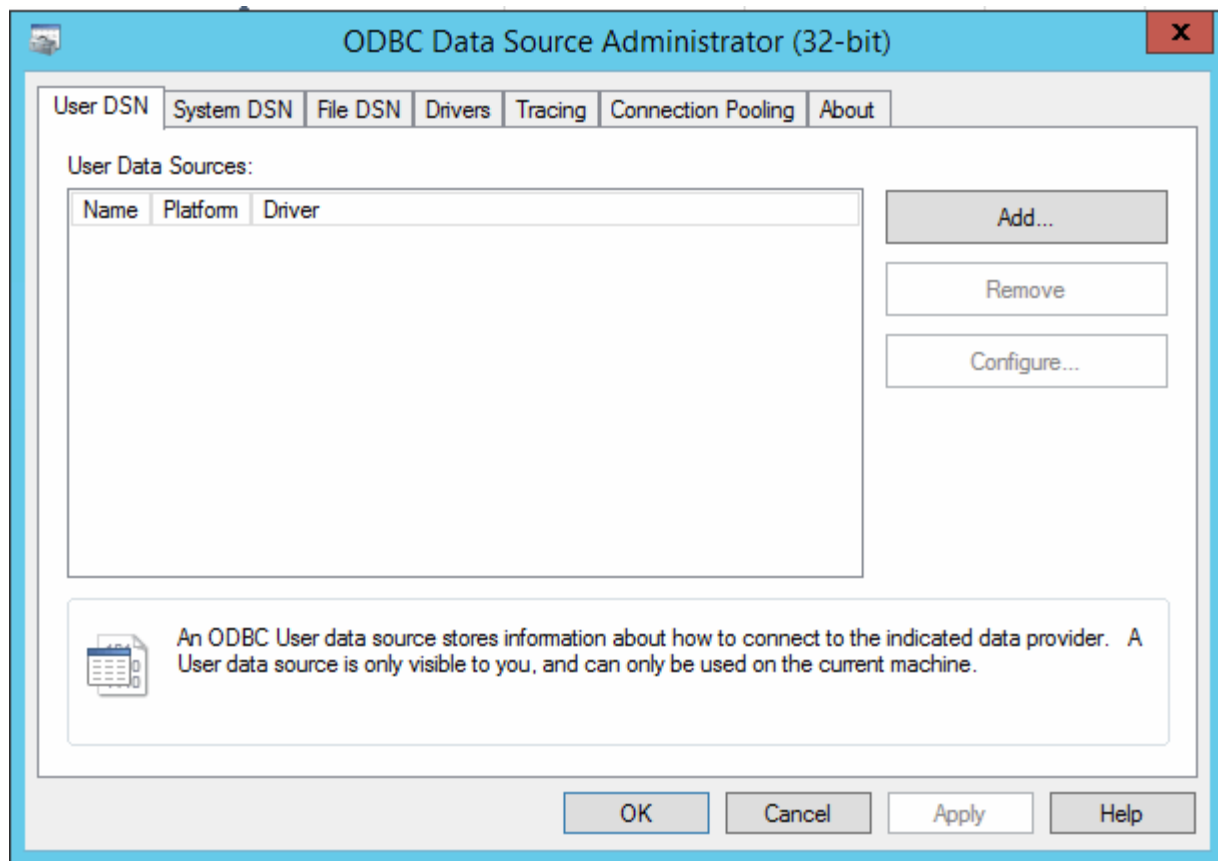
作業を開始する前に

管理者権限があるアカウントを使用してData Warehouseサーバへのリモートログインを実行する必要があります。

手順

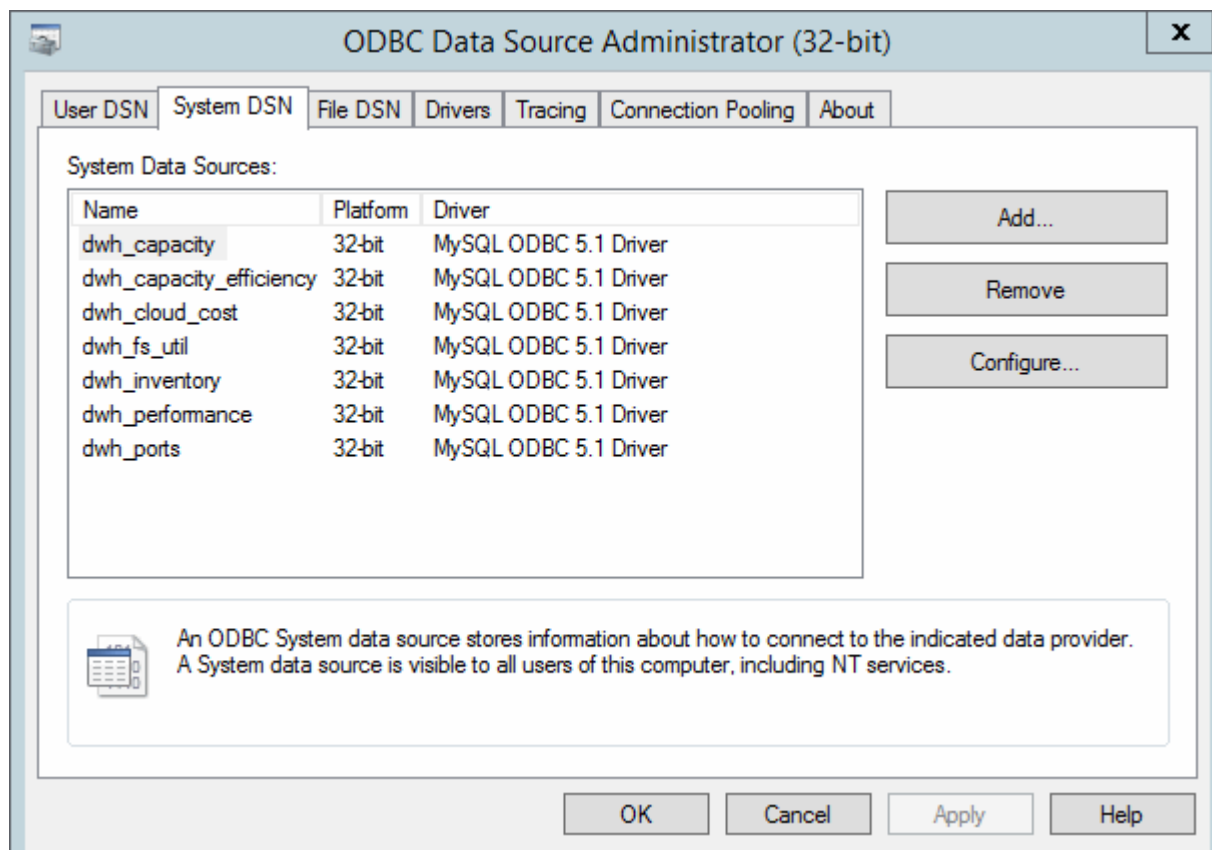
1. Data Warehouseをホストしているサーバへのリモートログインを実行します。
2. ODBC Administrationツールにアクセスします C:\Windows\SysWOW64\odbcad32.exe

[ODBC Data Source Administrator]画面が表示されます。



3. [システムDSN]\*をクリックします

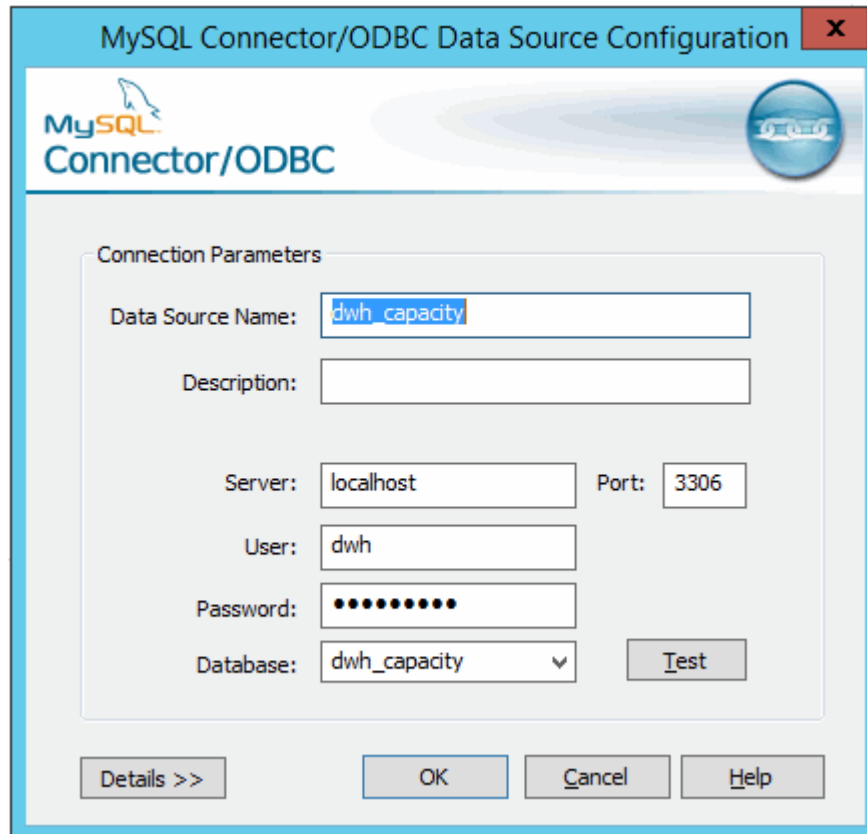
システムデータソースが表示されます。



4. リストからOnCommand Insight データソースを選択します。

5. [設定]\*をクリックします

[Data Source Configuration]画面が表示されます。



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. The main area is titled 'Connection Parameters' and contains several input fields: 'Data Source Name' (containing 'dwh\_capacity'), 'Description' (empty), 'Server' (containing 'localhost'), 'Port' (containing '3306'), 'User' (containing 'dwh'), 'Password' (containing masked characters), and 'Database' (a dropdown menu showing 'dwh\_capacity'). There is a 'Test' button next to the Database dropdown. At the bottom, there are four buttons: 'Details >>', 'OK', 'Cancel', and 'Help'.

6. [パスワード]\*フィールドに新しいパスワードを入力します。



## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。