Insight安全性(安全管理工具)

OnCommand Insight

NetApp
October 24, 2024

目录

securityadmin工具

OnCommand Insight提供的功能可使Insight环境在增强安全性的情况下运行。这些功能包括加密、密码哈希以及更改内部用户密码和用于加密和解密密码的密钥对的功能。您可以使用*SecurityAdmin Tool*在Insight环境中的所有服务器上管理这些功能。

什么是SecurityAdmin工具?

安全管理工具支持对存储内容进行更改、以及对OnCommand Insight安装进行协调更改。

SecurityAdmin工具的主要用途是安全配置(即存储)和密码的*Backup*和*Restore*。例如、您可以在本地采集单元上备份存储、然后在远程采集单元上还原该存储、从而确保整个环境中的密码协调。或者、如果您的环境中有多个OnCommand Insight服务器、则可能需要对服务器存储进行备份、并将其还原到其他服务器、以使密码保持不变。以下只是使用SecurityAdmin确保环境中的凝聚力的两个示例。

强烈建议在备份OnCommand Insight数据库时*备份存储*。否则可能导致无法访问。

该工具提供*交互*和*命令行*两种模式。

许多SecurityAdmin Tool操作都会更改存储的内容、同时也会更改安装、以确保存储和安装保持同步。

例如、

- 更改Insight用户密码后、SANscreen .Users表中的用户条目将使用新哈希进行更新。
- 当您更改MySQL用户的密码时、将执行相应的SQL语句来更新MySQL实例中用户的密码。

在某些情况下、会对安装进行多项更改：

- 修改dwh MySQL用户时、除了更新MySQL数据库中的密码之外、还将更新ODBC的多个注册表条目。

在以下各节中、"协调的变更"一词用于描述这些变更。

执行模式

- 正常/默认操作- SANscreen服务器服务必须正在运行

  对于默认执行模式，安全管理工具要求* SANscreen服务器服务*正在运行。该服务器用于身份验证、并通过调用该服务器对安装进行许多协调的更改。

- 直接操作- SANscreen服务器服务可能正在运行或已停止。

  在OCI服务器或DWH安装上运行时、该工具也可以在"直接"模式下运行。在此模式下、使用数据库执行身份验证和协调更改。未使用服务器服务。

  操作与普通模式相同、但有以下例外：

- 只有非域管理员用户才支持身份验证。(其密码和角色位于数据库中、而不是LDAP中的用户)。
- 不支持"替换密钥"操作。

- 已跳过存储还原的重新加密步骤。
- 恢复模式即使无法同时访问服务器和数据库(例如、由于存储中的root密码不正确)、该工具也可能会运行。

  在此模式下运行时、无法进行身份验证、因此无法执行对安装进行协调更改的操作。

  恢复模式可用于：

- 确定哪些存储条目错误(使用验证操作)
- 将不正确的root密码替换为正确的值。(这不会更改密码。用户必须输入当前密码。)

> 如果存储中的根密码不正确、并且密码未知、并且没有使用正确根密码的存储备份、则无法使用SecurityAdmin工具恢复安装。恢复安装的唯一方法是按照中所述的过程重置MySQL实例的密码 https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html。执行重置过程后、请使用CORRECE-STORE-password操作将新密码输入到存储中。

命令

不受限制的命令

不受限制的命令会对安装进行任何协调更改(信任存储库除外)。可以在不进行用户身份验证的情况下执行不受限制的命令。

命令	Description
备份存储	生成包含库的zip文件。库文件的相对路径将与相对于安装根的库路径匹配。 • Wildfly/standalone/configuration/vault/* • acq/conf/vault/* 请注意、强烈建议您在备份OnCommand Insight数据库时备份存储。
Check for－default-keys (检查默认密钥)	检查库的密钥是否与7.3.16之前实例中使用的默认库的密钥匹配。
CORRECE-STORE-password	将存储在存储中的(不正确)密码替换为用户已知的正确密码。 当库和安装不一致时、可以使用此选项。请注意，它不会更改安装中的实际密码。
	change-trust store-password更改用于信任存储的密码、并将新密码存储在存储中。信任存储库的当前密码必须为"已知"。

verify-keyStore	检查库中的值是否正确： • 对于OCI用户、密码哈希是否与数据库中的值匹配 • 对于MySQL用户、是否可以建立数据库连接 • 对于密钥库、是否可以加载密钥库并读取其密钥(如果有)
列表键	列出存储中的条目(不显示存储值)

受限命令

对安装进行协调更改的任何非隐藏命令都需要进行身份验证：

命令	Description
Restore-vault-backup	将当前存储替换为指定存储备份文件中包含的存储。 执行所有协调操作以更新安装、使其与还原的存储中的密码匹配： • 更新OCI通信用户密码 • 更新MySQL用户密码、包括root用户密码 • 对于每个密钥库、如果密钥库密码为"已知"、请使用还原的存储中的密码更新密钥库。 在正常模式下运行时、还会从实例中读取每个加密值、使用当前存储的加密服务对其解密、使用还原的存储的加密服务对其重新加密、并存储重新加密的值。
与存储同步	执行所有协调操作以更新安装、使其与还原的存储中的用户密码匹配： • 更新OCI通信用户密码 • 更新MySQL用户密码、包括root用户密码
change-password	更改存储中的密码并执行协调操作。
更换键	生成新的空库(将与现有库具有不同的密钥)。然后将条目从当前库复制到新库。然后从实例中读取每个加密值、使用当前存储的加密服务对其解密、使用还原的存储的加密服务对其重新加密、并存储重新加密的值。

协调行动

服务器存储

内部	更新数据库中用户的密码哈希

采集	更新数据库中用户的密码哈希 如果存在采集库、还应更新采集库中的条目
dwh_internal	更新数据库中用户的密码哈希
Cognos_admin	更新数据库中用户的密码哈希 如果是dwh和windows、请更新cognos/Cognos/Analytics /configuration/SANscreenAP.properties以将SANscreen属性设置为密码。
root	执行SQL以更新MySQL实例中的用户密码
清单	执行SQL以更新MySQL实例中的用户密码
dwh	执行SQL以更新MySQL实例中的用户密码 如果是DWH和Windows、请更新Windows注册表、将以下ODBC相关条目设置为新密码： • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity \PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity效率\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_FS_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Inventory\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_SEALIY\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_ports\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Cloud成本\PWD
dwhuser	执行SQL以更新MySQL实例中的用户密码

主机	执行SQL以更新MySQL实例中的用户密码
密钥库密码	使用新密码(Wildfly/standalone/configuration/server.keyore)重新写入密钥库
信任store_password	使用新密码(Wildfly/standalone/configuration/server.trunstore)重新写入密钥库
key_password	使用新密码(Wildfly/standalone/configuration/sso.jks)重新写入密钥库
Cognos_archive	无

采集存储

采集	无
信任store_password	使用新密码(如果存在)重新写入密钥库- acq/conf/cert/client.keyore

运行安全管理工具-命令行

在命令行模式下运行SA工具的语法为：

```
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
```

注意：

- 命令行上可能不存在"-i"选项(因为这会选择交互模式)。
- 对于"-s"和"-au"选项：
  - RAU不允许使用"-s"
  - DWH不允许使用"-au"

- 如果两者都不存在、则
  - 已在服务器、DWH和双上选择服务器存储
  - 在RAU上选择采集库
- lu和-lp选项用于用户身份验证。
  - 如果指定了<user>而未指定<password>、则系统将提示用户输入密码。
  - 如果未提供<user>且需要进行身份验证、则系统将提示用户输入<user>和<password>。

命令：

命令	使用情况
CORRECE-STORE-password	`securityadmin [-s`
-au] [-db] -pt <key> [<value>] `where` -pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value 	备份存储
`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> 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
备份存储	`securityadmin [-s`

-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ```	列表键
`` securityadmin [-s ```	-au] [-db] -l where -l specified command ```
检查键	``` securityadmin [-s ```
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ```	verify-keyStore (服务器)
`` securityadmin [-s] [-db] -v where -v specified command ```	升级

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted ``
更换键	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	Restore-vault-backup
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``
change-password (服务器)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]` `where` `-up specified command ("update-password")` `-un <user> entry ("user") name to update` `-p <password> new password. If <password not supplied, user will be prompted.` `-sh for mySQL user, use strong hash`

采集用户的change-password (采集)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]` `where` `-up specified command ("update-password") -p <password> new password. If <password not supplied, user will be prompted.`
信任存储库-_password的change-password (采集)	`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.`
与存储同步(服务器)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>` `where` `-sv specified command`

运行安全管理工具-交互模式

交互式-主菜单

要以交互模式运行SA工具、请输入以下命令：

```
securityadmin -i
```

在服务器或双重安装中、`SecurityAdmin`将提示用户选择服务器或本地采集单元。

检测到服务器和采集单元节点！选择需要重新配置其安全性的节点：

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

在DWH上、系统会自动选择"服务器"。在远程AU上、将自动选择"Acquisition Unit"。

交互式-服务器：root密码恢复

在服务器模式下、SecurityAdmin Tool将首先检查存储的root密码是否正确。否则、该工具将显示root密码恢复屏幕。

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

如果选择选项1、系统将提示用户输入正确的密码。

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
```

如果输入的密码正确、则会显示以下内容。

```
 Password verified.  Vault updated
```

按ENTER键将显示服务器不受限制的菜单。

如果输入的密码不正确、则会显示以下内容

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```

按ENTER键将返回恢复菜单。

如果选择选项2、系统将提示用户提供要从中读取正确密码的备份文件的名称：

```
 Enter Backup File Location:
```
如果备份密码正确、则会显示以下内容。

```
 Password verified.  Vault updated
```
按ENTER键将显示服务器不受限制的菜单。

如果备份中的密码不正确、则会显示以下内容

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```
按ENTER键将返回恢复菜单。

交互式-服务器：正确的密码

"正确密码"操作用于更改存储在库中的密码、使其与安装所需的实际密码匹配。如果安装更改是通过非安全管理工具进行的、则此命令非常有用。示例包括：

- 通过直接访问MySQL修改了SQL用户的密码。
- 使用keytool替换密钥库或更改密钥库的密码。
- OCI数据库已还原、该数据库的内部用户密码不同

"正确密码"将首先提示用户选择用于存储正确值的密码。

```
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:
```

选择要更正的条目后、系统会提示用户输入希望如何提供该值。

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

如果选择选项1、系统将提示用户输入正确的密码。

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
```

如果输入的密码正确、则会显示以下内容。

```
 Password verified.  Vault updated
```

按ENTER键将返回到服务器不受限制的菜单。

如果输入的密码不正确、则会显示以下内容

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

按ENTER键将返回到服务器不受限制的菜单。

如果选择选项2、系统将提示用户提供要从中读取正确密码的备份文件的名称：

```
 Enter Backup File Location:
```

如果备份密码正确、则会显示以下内容。

```
 Password verified.  Vault updated
```

按ENTER键将显示服务器不受限制的菜单。

如果备份中的密码不正确、则会显示以下内容

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

按ENTER键将显示服务器不受限制的菜单。

交互式-服务器：验证存储内容

验证存储内容将检查存储是否具有与使用早期OCI版本分发的默认存储匹配的密钥、并检查存储中的每个值是否与安装匹配。

每个密钥的可能结果如下：

确定	存储值正确
未选中	不能根据安装检查此值

差	此值与安装不匹配
缺少	缺少预期条目。

```
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
```

交互式-服务器：备份

备份将提示输入备份zip文件应存储到的目录。目录必须已存在、文件名将为ServerSecurityBackup-yyyyy-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
```

交互式-服务器：登录

登录操作用于对用户进行身份验证、并获得对修改安装的操作的访问权限。用户必须具有管理Privileges。在服务器上运行时、可以使用任何管理员用户；在直接模式下运行时、该用户必须是本地用户、而不是LDAP用户。

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

或

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

如果密码正确且用户是管理员用户、则会显示受限菜单。

如果密码不正确、将显示以下内容：

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

如果用户不是管理员、则会显示以下内容：

```
Authenticating via server. Enter user and password

UserName: user

Password:

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

交互式-服务器：受限菜单

用户登录后、该工具将显示受限菜单。

```
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:
```

交互式-服务器：更改密码

"更改密码"操作用于将安装密码更改为新值。

"Change Password"(更改密码)将首先提示用户选择要更改的密码。

```
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:
```

选择要更正的条目后、如果用户是MySQL用户、系统将询问该用户是否对密码进行强哈希

```
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
```

接下来、系统会提示用户输入新密码。

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

Password is empty - cancelling operation
```

如果输入非空密码、系统将提示用户确认该密码。

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

如果更改失败、则会显示错误或异常。

交互式-服务器：还原

交互式-服务器：更改加密密钥

更改加密密钥操作将替换用于加密存储条目的加密密钥、并替换用于存储加密服务的加密密钥。由于加密服务的密钥已更改、因此数据库中的加密值将重新加密；这些值将被读取、使用当前密钥解密、使用新密钥加密并保存回数据库。

在直接模式下不支持此操作、因为服务器会为某些数据库内容提供重新加密操作。

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

交互式-服务器：修复安装

修复安装操作将更新安装。除root用户之外、所有可通过安全管理工具更改的安装密码都将设置为库中的密码。

- OCI内部用户的密码将会更新。
- 系统将更新MySQL用户的密码(root用户除外)。
- 密钥库的密码将被更新。

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

Confirm:  (y/N): y

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

此操作将在首次更新失败时停止、并显示错误或异常。

管理Insight服务器上的安全性

。 `securityadmin` 使用工具可以管理Insight服务器上的安全选项。安全管理包括更改密码、生成新密钥、保存和还原您创建的安全配置或将配置还原为默认设置。

关于此任务

您可以使用 `securityadmin` 用于管理安全性的工具：

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

有关详细信息、请参见"安全管理员"文档。

管理本地采集单元上的安全性

。 `securityadmin` 使用工具可以管理本地采集用户(LAU)上的安全选项。安全管理包括管理密钥和密码、保存和还原您创建的安全配置或将配置还原为默认设置。

开始之前

您必须拥有 `admin` 执行安全配置任务的权限。

关于此任务

您可以使用 `securityadmin` 用于管理安全性的工具：

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

有关详细信息、请参见"securityadmin工具"说明。

管理RAU上的安全性

。 `securityadmin` 使用工具可以管理RAU上的安全选项。您可能需要备份或还原存储配置、更改加密密钥或更新采集单元的密码。

关于此任务

您可以使用 `securityadmin` 用于管理安全性的工具：

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

更新LAU/RAU安全配置的一种情形是、在服务器上更改了"采集"用户的密码后、更新该用户的密码。LAu和所有RAus使用与服务器"采集"用户相同的密码与服务器进行通信。

"采集"用户仅存在于Insight服务器上。RAU或LAU在连接到服务器时以该用户身份登录。

有关详细信息、请参见"securityadmin工具"说明。

管理数据仓库上的安全性

。 `securityadmin` 您可以使用工具管理数据仓库服务器上的安全选项。安全管理包括更新DWH服务器上内部用户的内部密码、创建安全配置的备份或将配置还原为默认设置。

关于此任务

您可以使用 `securityadmin` 用于管理安全性的工具：

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

有关详细信息、请参见"安全管理员"文档。

更改OnCommand Insight 内部用户密码

安全策略可能要求您更改OnCommand Insight 环境中的密码。一台服务器上的某些密码存在于环境中的另一台服务器上、要求您更改这两台服务器上的密码。例如、在Insight服务器上更改"`inventory`"用户密码时、必须与为该Insight服务器配置的Data Warehouse server Connector上的"`inventory`"用户密码匹配。

开始之前

在更改密码之前、您应了解用户帐户的依赖关系。如果未更新所有所需服务器上的密码、则Insight组件之间的通信将失败。

关于此任务

下表列出了Insight服务器的内部用户密码、并列出了具有需要与新密码匹配的相关密码的Insight组件。

Insight服务器密码	所需更改

内部	
采集	LAU、RAU
dwh_internal	数据仓库
主机	
清单	数据仓库
root	

下表列出了数据仓库的内部用户密码、并列出了具有需要与新密码匹配的相关密码的Insight组件。

数据仓库密码	所需更改
Cognos_admin	
dwh	
dwh_internal (使用服务器连接器配置UI进行更改)	Insight服务器
dwhuser	
主机	
清单(使用Server Connector配置UI进行更改)	Insight服务器
root	

在**DWH**服务器连接配置用户界面中更改密码

下表列出了LAU的用户密码、并列出了具有需要与新密码匹配的相关密码的Insight组件。

LAU密码	所需更改
采集	Insight服务器、RAU

使用服务器连接配置**UI**更改"清单"和"**dwh_interne**"密码

如果您需要更改"`inventory`"或`dwh_internal`"密码以匹配Insight服务器上的密码、请使用数据仓库UI。

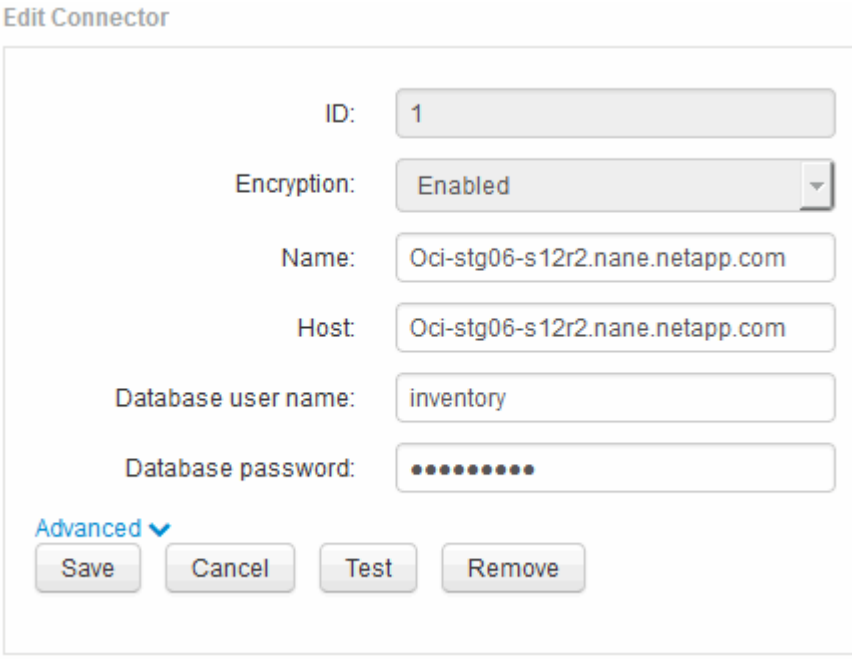
开始之前

要执行此任务、您必须以管理员身份登录。

步骤

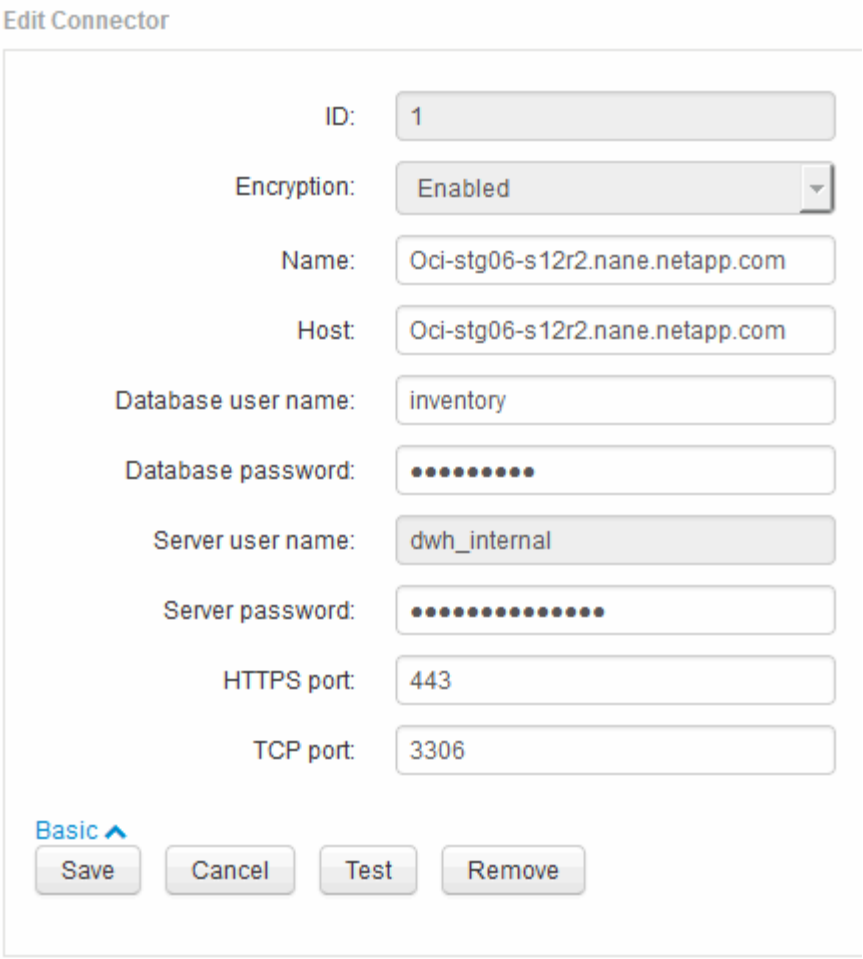
1. 登录到数据仓库门户、网址为 https://hostname/dwh、其中hostname是安装了OnCommand Insight 数据仓库的系统的名称。
2. 从左侧导航窗格中、单击*连接器*。

   此时将显示*编辑连接器*屏幕。



3. 为*数据库密码*字段输入新的"`inventory`"密码。
4. 单击 * 保存 * 。
5. 要更改`dwh_internal`密码、请单击*高级。*

   此时将显示编辑连接器高级屏幕。



6. 在*服务器密码*字段中输入新密码：
7. 单击保存。

使用ODBC管理工具更改dwh密码

在Insight服务器上更改dwh用户的密码时、还必须在数据仓库服务器上更改此密码。您可以使用ODBC数据源管理员工具更改数据仓库上的密码。

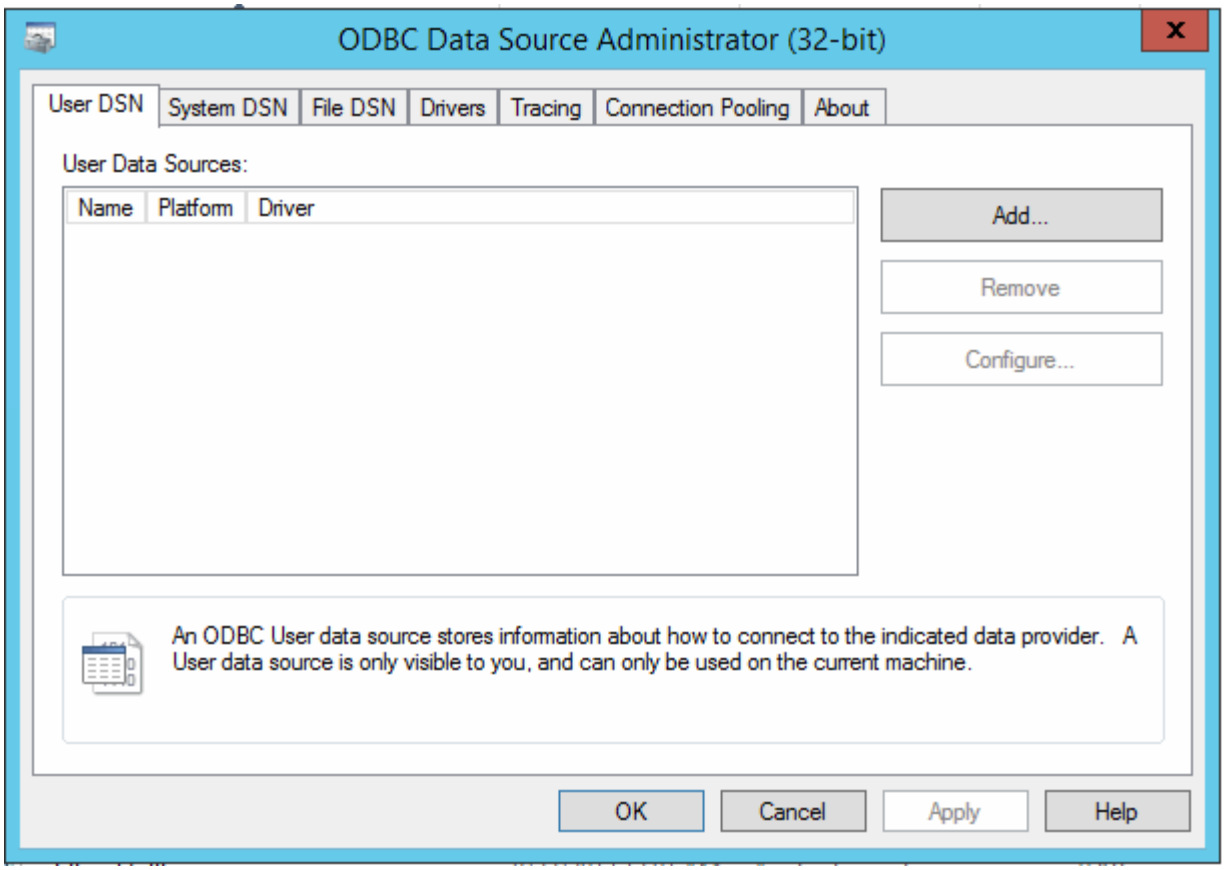
开始之前

您必须使用具有管理员权限的帐户远程登录到数据仓库服务器。

步骤

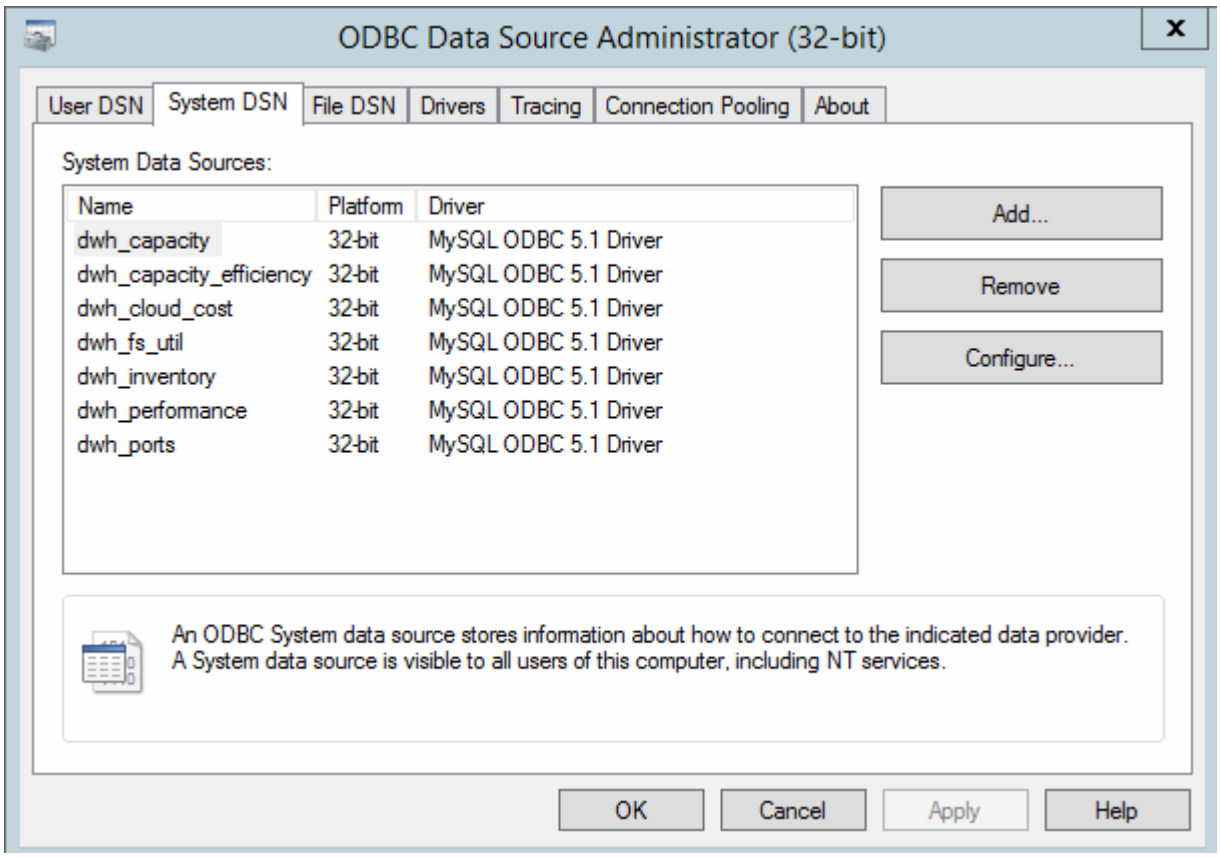
1. 远程登录到托管该数据仓库的服务器。
2. 访问ODBC管理工具、网址为 `C:\Windows\SysWOW64\odbcad32.exe`

   系统将显示"ODBC数据源管理员"屏幕。



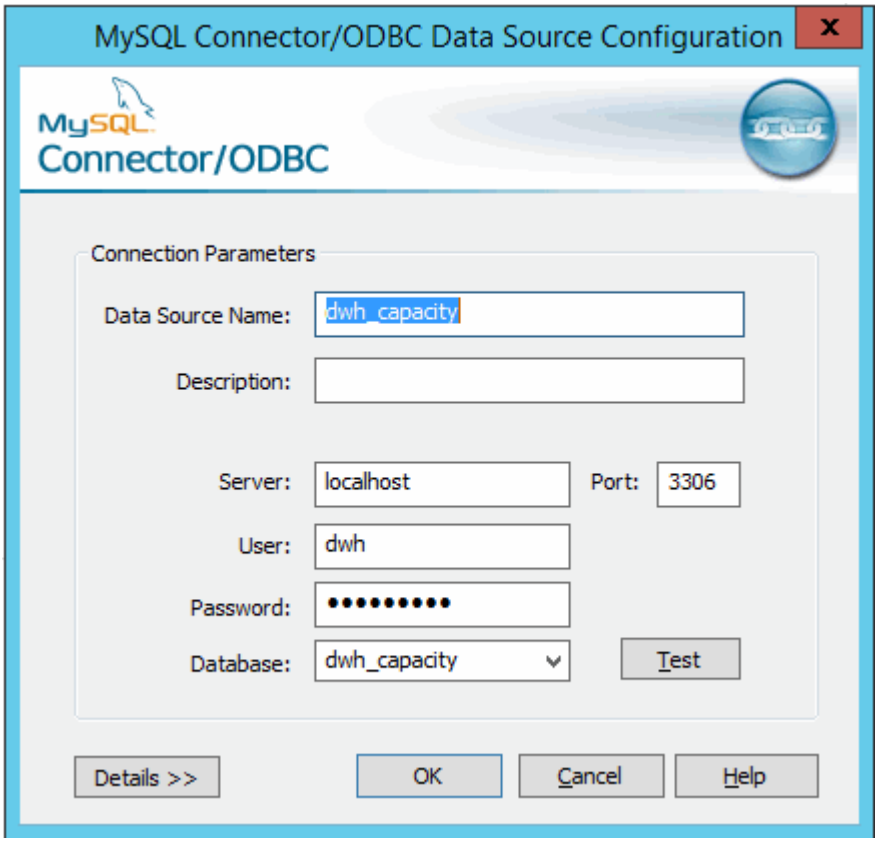
3. 单击*系统DSN*

   此时将显示系统数据源。



4. 从列表中选择一个OnCommand Insight 数据源。
5. 单击*配置*

   此时将显示Data Source Configuration屏幕。



6. 在*密码*字段中输入新密码。