Insight Security

OnCommand Insight

NetApp
October 24, 2024

目錄

Insight Security

OnCommand Insight 提供的功能可讓 Insight 環境以增強的安全性運作。這些功能包括加密、密碼雜湊、以及變更內部使用者密碼和密碼加密和解密金鑰配對的能力。您可以使用 securityadmin Tool 在 Insight 環境中的所有伺服器上管理這些功能。

什麼是安全性管理工具？

安全性管理工具支援變更資料保險箱的內容、以及協調一致地變更 OnCommand Insight 安裝。

安全性管理工具的主要用途是 * 備份 * 和 * 還原 * 安全性組態（即資料保險箱）和密碼。例如、您可以在本機擷取單元上備份資料保險箱、並在遠端擷取單元上還原資料保險箱、確保整個環境都能協調密碼。或者、如果您的環境中有多部 OnCommand Insight 伺服器、您可能需要備份伺服器資料保險箱、並將其還原至其他伺服器、以保持密碼相同。以下只是安全性管理可用於確保環境內凝聚力的兩個範例。

強烈建議您在備份 OnCommand Insight 資料庫時 * 備份資料保險箱 * 。否則可能導致存取中斷。

此工具同時提供 * 互動 * 和 * 命令列 * 模式。

許多 securityadmin Tool 作業會變更資料保險箱的內容、也會變更安裝、確保資料保險箱和安裝保持同步。

例如、

- 當您變更 Insight 使用者密碼時、 SANscreen 。 Users 表格中的使用者項目將會以新的雜湊更新。
- 當您變更 MySQL 使用者密碼時、將會執行適當的 SQL 陳述式、以更新 MySQL 執行個體中的使用者密碼。

在某些情況下、會對安裝進行多項變更：

- 修改 dwh MySQL 使用者時、除了更新 MySQL 資料庫中的密碼之外、也會更新多個 ODBC 登錄項目。

在下列各節中、使用「協調式變更」一詞來描述這些變更。

執行模式

- 正常 / 預設操作 - SANscreen 伺服器服務必須執行

  對於默認執行模式， securityadmin Tool 要求 SANscreen 服務器服務 * 正在運行。伺服器用於驗證、許多協調一致的安裝變更都是透過呼叫伺服器來進行。

- 直接操作 - SANscreen 伺服器服務可能正在執行或停止。

  在 OCI 伺服器或 DWH 安裝上執行時、工具也可以在「直接」模式下執行。在此模式中、驗證和協調變更是使用資料庫來執行。未使用伺服器服務。

  操作與一般模式相同、但有下列例外：

- 驗證僅支援非網域管理員使用者。（密碼和角色位於資料庫中的使用者、而非 LDAP ）。
- 不支援「置換金鑰」操作。

- 會略過資料保險箱還原的重新加密步驟。
- 恢復模式即使無法同時存取伺服器和資料庫、也可能執行此工具（例如、因為資料保險箱中的根密碼不正確）。

  在此模式下執行時、無法進行驗證、因此無法執行協調變更安裝的作業。

  恢復模式可用於：

- 判斷哪些資料保險箱項目錯誤（使用驗證作業）
- 請以正確的值取代不正確的根密碼。（這不會變更密碼。使用者必須輸入目前的密碼。）

> ⓘ 如果資料保險箱中的根密碼不正確、而且密碼未知、而且沒有正確的根密碼備份資料保險箱、則無法使用 securityadmin Tool 還原安裝。恢復安裝的唯一方法是按照中介紹的步驟重置 MySQL 實例的密碼 https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html。執行重設程序後、請使用正確的儲存密碼操作、將新密碼輸入資料保險箱。

命令

無限制命令

無限制命令會對安裝進行任何協調的變更（信任存放區除外）。不受限制的命令可在不進行使用者驗證的情況下執行。

命令	說明
備份資料保險箱	建立包含資料保險箱的 zip 檔案。至資料保險箱檔案的相對路徑將與相對於安裝根目錄的資料保險箱路徑相符。 • Wildfly / 獨立 / 組態 / 資料保險箱 / * • ACQ/conf/vVault/*
檢查預設金鑰	檢查資料保險箱的金鑰是否與 7.3.16 之前版本中使用的預設資料保險箱金鑰相符。
正確儲存的密碼	以使用者已知的正確密碼取代儲存在資料保險箱中的（不正確）密碼。 當資料保險箱和安裝不一致時、可能會使用此選項。* 請注意、它不會變更安裝中的實際密碼。 *
change-trust 儲存區密碼	變更用於信任存放區的密碼、並將新密碼儲存在資料保險箱中。信任存放區的目前密碼必須為「已知」。

驗證 Keystore	檢查資料保險箱中的值是否正確： • 對於 OCI 使用者、密碼雜湊是否與資料庫中的值相符 • 對於 MySQL 使用者、可以建立資料庫連線 • 對於 Keystore 、是否可以載入 Keystore 及其金鑰（如果有）讀取
清單鍵	列出資料保險箱中的項目（不顯示儲存的值）

受限命令

任何對安裝進行協調變更的非隱藏命令都需要驗證：

命令	說明
還原資料保險箱備份	以包含在指定資料保險箱備份檔案中的資料保險箱取代目前的資料保險箱。 執行所有協調的動作來更新安裝以符合還原資料保險箱中的密碼： • 更新 OCI 通訊使用者密碼 • 更新 MySQL 使用者密碼、包括 root • 對於每個 Keystore 、如果 Keystore 密碼為「已知」、請使用還原資料保險箱中的密碼來更新 Keystore 。 以正常模式執行時、也會從執行個體讀取每個加密值、使用目前資料保險箱的加密服務將其解密、使用還原的資料保險箱加密服務重新加密、以及儲存重新加密的值。
與資料保險箱同步	執行所有協調的動作來更新安裝，以符合還原資料保險箱中的使用者密碼： • 更新 OCI 通訊使用者密碼 • 更新 MySQL 使用者密碼、包括 root
變更密碼	變更資料保險箱中的密碼並執行協調的動作。
置換鍵	建立新的空資料保險箱（其金鑰與現有的資料保險箱不同）。然後將項目從目前的資料保險箱複製到新的資料保險箱。然後從執行個體讀取每個加密值、使用目前資料保險箱的加密服務將其解密、使用還原的資料保險箱加密服務重新加密、並儲存重新加密的值。

隱藏命令

SA 工具提供下列命令、這些命令不需要驗證、但必須對安裝進行協調的變更。

清單金鑰升級（伺服器）	如果使用者尚未驗證、請使用目前資料保險箱中的內部帳戶和密碼進行驗證。然後以備份檔案中的資料保險箱取代目前的資料保險箱，並執行協調的動作。
升級（併購）	以備份檔案中的資料保險箱取代目前的資料保險箱，並執行協調的動作。

協調行動

伺服器資料保險箱

內部_	更新資料庫中使用者的密碼雜湊
併購	更新資料庫中使用者的密碼雜湊 如果有擷取資料保險箱、請同時更新擷取資料保險箱中的項目
dwh_internal	更新資料庫中使用者的密碼雜湊
Cogns_admin	更新資料庫中使用者的密碼雜湊 如果是 DWH 和 Windows 、請更新 SANscreen / Cognos / 分析 / 組態 / SANscreenAP.properties 、將 Cognos ・ admin 屬性設定為密碼。
根	執行 SQL 以更新 MySQL 執行個體中的使用者密碼
庫存	執行 SQL 以更新 MySQL 執行個體中的使用者密碼

dwh	執行 SQL 以更新 MySQL 執行個體中的使用者密碼 如果是 DWH 和 Windows 、請更新 Windows 登錄、將下列與 ODBC 相關的項目設定為新密碼： • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_capies\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_capal_Efficiation\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_Performance \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	執行 SQL 以更新 MySQL 執行個體中的使用者密碼
主機	執行 SQL 以更新 MySQL 執行個體中的使用者密碼
Keystore 密碼	使用新密碼重新寫入金鑰儲存區： wildfly/standbed/configuration/server.keystore
truststore_password	使用新密碼重新寫入金鑰儲存區： wildfly/standbed/configuration/server.trustore
key_password	使用新密碼重新寫入金鑰儲存區： wildfly/standbed/configuration/sso.jks
Cognos 歸檔	無

擷取 **Vault**

併購	無

truststore_password	使用新密碼（如果存在）重新寫入密鑰庫 - acq/conf/cert / client.keystore

執行安全管理工具 - 命令列

在命令列模式中執行 SA 工具的語法如下：

```
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
```

附註：

- 命令列上可能沒有「 -I 」選項（因為這會選取互動模式）。
- 對於 "-s" 和 "-au" 選項：
  - Rau 不允許使用 "-s"
  - DWH 不允許使用 "-au"
  - 如果兩者都不存在、則
    - 伺服器資料保險箱是在伺服器、 DWH 和雙工上選取
    - 擷取資料保險箱是在 Rau 上選取
- Lu 和 -lp 選項用於使用者驗證。
  - 如果已指定 <user> 且未指定 <password> 、則系統會提示使用者輸入密碼。
  - 如果未提供 <user> 且需要驗證、則系統會提示使用者輸入 <user> 和 <password> 。

命令：

命令	使用量

正確儲存的密碼	`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
 	
` `
	備份資料保險箱

`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 ` `
備份資料保險箱	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ` `	清單鍵

`securityadmin [-s`	-au] [-db] -l where -l specified command ``
檢查鍵	`securityadmin [-s`
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ``	VERIF-keystore （伺服器）

`securityadmin [-s] [-db] -v`
 	
`where`
 	
`-v specified command`
	升級

`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 ``

置換鍵	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	還原資料保險箱備份
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``

變更密碼（伺服器）	`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`

擷取使用者的變更密碼（擷取）	`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.`

truststore—_password 的 change-password （取得）	`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.`

與資料保險箱同步（伺服器）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

執行安全管理工具 - 互動模式

互動式 - 主功能表

若要以互動模式執行 SA 工具、請輸入下列命令：

```
 securityadmin -i
```

在伺服器或雙安裝上、 `securityadmin` 會提示使用者選擇伺服器或本機擷取單元。

偵測到伺服器和擷取單元節點！選取需要重新設定安全性的節點：

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

在 DWH 上、會自動選取「伺服器」。在遠端 AU 上、系統會自動選取「擷取單元」。

互動式 - 伺服器：根密碼還原

在伺服器模式中、 securityadmin Tool 會先檢查儲存的根密碼是否正確。如果沒有、工具會顯示 root 密碼恢復畫面。

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

如果選擇選項 1 、系統會提示使用者輸入正確的密碼。

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

如果輸入正確的密碼、將會顯示下列內容。

```
 Password verified.  Vault updated
```

按下 `ENTER` 會顯示伺服器不受限制的功能表。

如果輸入的密碼錯誤、將會顯示下列內容

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

按下 `ENTER` 會返回恢復功能表。

如果選取選項 2 、系統會提示使用者提供備份檔案的名稱、以便從中讀取正確的密碼：

```
 Enter Backup File Location:
```

如果備份的密碼正確、則會顯示下列內容。

```
 Password verified.  Vault updated
```

按下 `ENTER` 會顯示伺服器不受限制的功能表。

如果備份中的密碼不正確、則會顯示下列內容

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```
按下 `ENTER` 會返回恢復功能表。

互動式 - 伺服器：正確密碼

「正確密碼」動作用於變更儲存在資料保險箱中的密碼、使其符合安裝所需的實際密碼。此命令在安全性管理工具以外的地方變更安裝時非常有用。範例包括：

- SQL 使用者的密碼是透過直接存取 MySQL 來修改的。
- 使用 keytool 替換密鑰庫或更改密鑰庫的密碼。
- OCI 資料庫已還原、且該資料庫有不同的內部使用者密碼

「正確密碼」會先提示使用者選擇要儲存正確值的密碼。

```
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:
```

選取要修正的項目之後、系統會提示使用者提供值的方式。

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

如果選擇選項 1 、系統會提示使用者輸入正確的密碼。

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

如果輸入正確的密碼、將會顯示下列內容。

```
 Password verified.  Vault updated
```

按下 `ENTER` 會返回伺服器不受限制的功能表。

如果輸入的密碼錯誤、將會顯示下列內容

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

按下 ENTER 會返回伺服器不受限制的功能表。

如果選取選項 2 、系統會提示使用者提供備份檔案的名稱、以便從中讀取正確的密碼：

```
 Enter Backup File Location:
```

如果備份的密碼正確、則會顯示下列內容。

```
 Password verified.  Vault updated
```

按下 `ENTER` 會顯示伺服器不受限制的功能表。

如果備份中的密碼不正確、則會顯示下列內容

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

按下 ENTER 會顯示伺服器不受限制的功能表。

互動式 - 伺服器：驗證 **Vault** 內容

確認 Vault 內容會檢查資料保險箱是否有與以舊版 OCI 發佈的預設資料保險箱相符的金鑰、並檢查資料保險箱中的每個值是否與安裝相符。

每個關鍵字的可能結果如下：

好的	資料保險箱值正確
未核取	無法對照安裝檢查此值

不良	此值與安裝不符
遺失	缺少預期的項目。

```
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
```

互動式 - 伺服器：備份

備份將提示輸入儲存備份 zip 檔案的目錄。目錄必須已存在、且檔案名稱為 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
```

互動式 - 伺服器：登入

登入動作用於驗證使用者、並存取修改安裝的作業。使用者必須擁有管理 Privileges 。與伺服器一起執行時、可以使用任何管理員使用者；在直接模式下執行時、使用者必須是本機使用者、而非 LDAP 使用者。

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

或

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

UserName: admin

Password:
```

如果密碼正確且使用者是管理員使用者、則會顯示受限功能表。

如果密碼不正確、則會顯示下列內容：

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

UserName: admin

Password:

Login Failed!
```

如果使用者不是管理員、則會顯示下列內容：

```
Authenticating via server. Enter user and password

UserName: user

Password:

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

互動式 - 伺服器：受限功能表

使用者登入後、工具會顯示「受限制的功能表」。

```
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:
```

互動式 - 伺服器：變更密碼

「變更密碼」動作用於將安裝密碼變更為新值。

「變更密碼」會先提示使用者選擇要變更的密碼。

```
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:
```

選取要修正的項目之後、如果使用者是 MySQL 使用者、系統會詢問使用者是否要加強密碼雜湊

```
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
```

接著、系統會提示使用者輸入新密碼。

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

Password is empty - cancelling operation
```

如果輸入非空密碼、系統會提示使用者確認密碼。

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

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

如果變更不成功、則會顯示錯誤或例外。

互動式 - 伺服器：還原

互動式 - 伺服器：變更加密金鑰

「變更加密金鑰」動作將取代用於加密資料保險箱項目的加密金鑰、並取代用於資料保險箱加密服務的加密金鑰。由於加密服務的金鑰已變更、因此資料庫中的加密值將會重新加密；這些值將會讀取、以目前金鑰解密、以新金鑰加密、並儲存回資料庫。

直接模式不支援此動作、因為伺服器會為某些資料庫內容提供重新加密作業。

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

Confirm (y/N): y

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

互動式 - 伺服器：修復安裝

「修復安裝」動作將會更新安裝。所有可透過安全管理工具變更的安裝密碼（ root 除外）都會設為資料保險箱中的密碼。

- 保監處內部使用者的密碼將會更新。
- MySQL 使用者的密碼（ root 除外）將會更新。
- Keystone 的密碼將會更新。

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

Confirm:  (y/N): y

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

此動作將在第一次不成功的更新時停止、並顯示錯誤或例外。

管理Insight伺服器上的安全性

。 `securityadmin` 工具可讓您管理Insight伺服器上的安全選項。安全管理包括變更密碼、產生新金鑰、儲存及還原您建立的安全組態、或將組態還原為預設設定。

關於這項工作

您可以使用 `securityadmin` 管理安全性的工具：

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

如需詳細資訊、請參閱"安全性管理"文件。

管理本地採購單位的安全性

。 `securityadmin` 此工具可讓您管理本機擷取使用者（Lau）的安全選項。安全管理包括管理金鑰和密碼、儲存及還原您建立的安全組態、或將組態還原為預設設定。

開始之前

您必須擁有 `admin` 執行安全組態工作的權限。

關於這項工作

您可以使用 `securityadmin` 管理安全性的工具：

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

如需詳細資訊、請參閱"安全性管理工具"指示。

管理Rau的安全性

。 `securityadmin` 工具可讓您管理Rous上的安全選項。您可能需要備份或還原資料保險箱組態、變更加密金鑰、或更新擷取單位的密碼。

關於這項工作

您可以使用 `securityadmin` 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 安全性組態的其中一個案例、是在伺服器上變更該使用者的密碼時、更新「取得」使用者密碼。Lau 和所有的 Raus 都使用與伺服器「取得」使用者相同的密碼來與伺服器通訊。

「擷取」使用者僅存在於Insight伺服器上。當Rau或Lau連線至伺服器時、會以該使用者的身分登入。

如需詳細資訊、請參閱"安全性管理工具"指示。

管理資料倉儲的安全性

。 `securityadmin` 工具可讓您管理資料倉儲伺服器上的安全選項。安全管理包括更新DWH伺服器上內部使用者的內部密碼、建立安全組態備份、或將組態還原為預設設定。

關於這項工作

您可以使用 `securityadmin` 管理安全性的工具：

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

如需詳細資訊、請參閱"安全性管理"文件。

變更OnCommand Insight 內部使用者密碼

安全性原則可能需要您在OnCommand Insight 您的環境中變更密碼。某部伺服器上的某些密碼存在於環境中的不同伺服器上、需要您變更兩部伺服器上的密碼。例如、當您變更Insight Server上的「Inventory」使用者密碼時、您必須符合Data倉儲伺服器Connector上針對該Insight Server所設定的「Inventory」使用者密碼。

開始之前

變更密碼之前、您應該先瞭解使用者帳戶的相依性。若未更新所有必要伺服器上的密碼、Insight元件之間的通訊將會失敗。

關於這項工作

下表列出Insight Server的內部使用者密碼、並列出具有相依密碼的Insight元件、這些元件必須符合新密碼。

Insight Server密碼	必要變更

內部_	
併購	劉羅
dwh_internal	資料倉儲
主機	
庫存	資料倉儲
根	

下表列出Data倉儲的內部使用者密碼、並列出Insight元件、這些元件的相依密碼必須與新密碼相符。

資料倉儲密碼	必要變更
Cogns_admin	
dwh	
Dwh_internal（使用伺服器連接器組態UI變更）	Insight伺服器
dwhuser	
主機	
庫存（使用伺服器連接器組態UI變更）	Insight伺服器
根	

*變更DWH伺服器連線組態Ui*中的密碼

下表列出了劉的使用者密碼、並列出了Insight元件、這些元件的相依密碼必須與新密碼相符。

劉密碼	必要變更
併購	Insight Server、Rau

使用伺服器連線組態**UI**變更「庫存」和「**dwh_internal**」密碼

如果您需要變更「Inventory」或「dwh_internal」密碼、以符合Insight伺服器上的密碼、請使用Data倉儲UI。

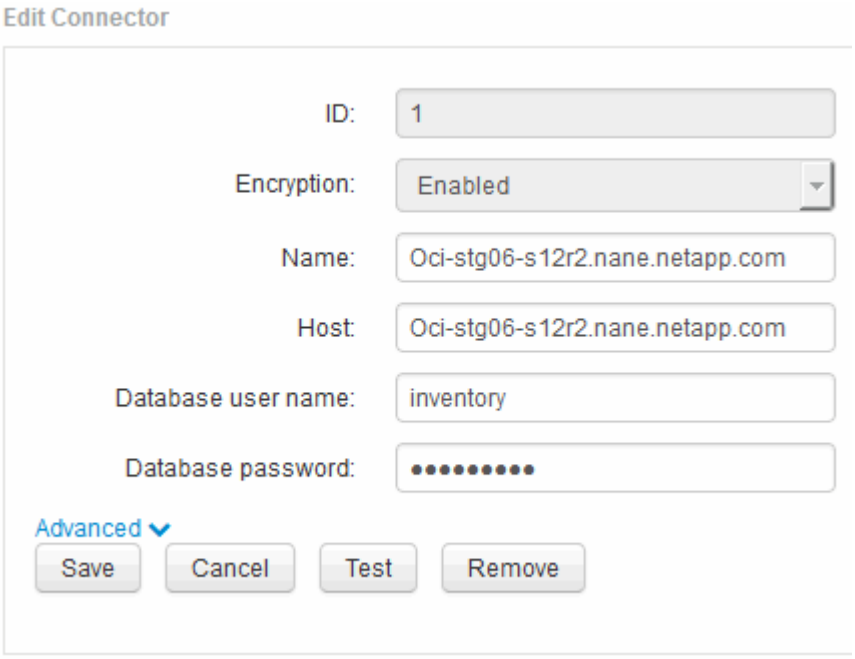
開始之前

您必須以系統管理員身分登入才能執行此工作。

步驟

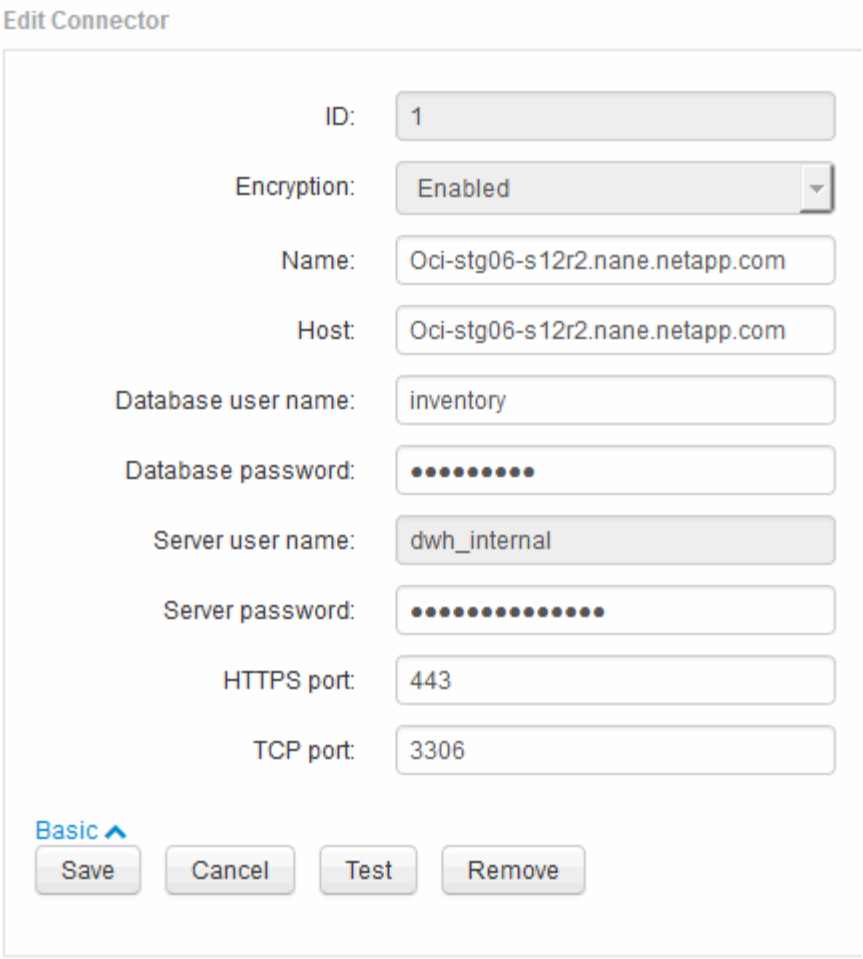
1. 登入資料倉儲入口網站： https://hostname/dwh、其中、主機名稱是OnCommand Insight 安裝了「IsorData倉儲」的系統名稱。
2. 在左側的導覽窗格中、按一下* Connectors *。

   此時將顯示*編輯連接器*畫面。



3. 在「資料庫密碼」欄位中輸入新的「'inventory'」密碼。
4. 按一下「儲存」
5. 若要變更「dwh_internal」密碼、請按一下*進階。*

   此時會顯示Edit Connector Advanced（編輯連接器進階）畫面。



6. 在*伺服器密碼*欄位中輸入新密碼：
7. 按一下儲存。

使用「ODBC管理」工具變更dwh密碼

當您在Insight伺服器上變更dwh使用者的密碼時、也必須在Data倉儲伺服器上變更密碼。您可以使用「ODBC資料來源管理員」工具來變更資料倉儲上的密碼。

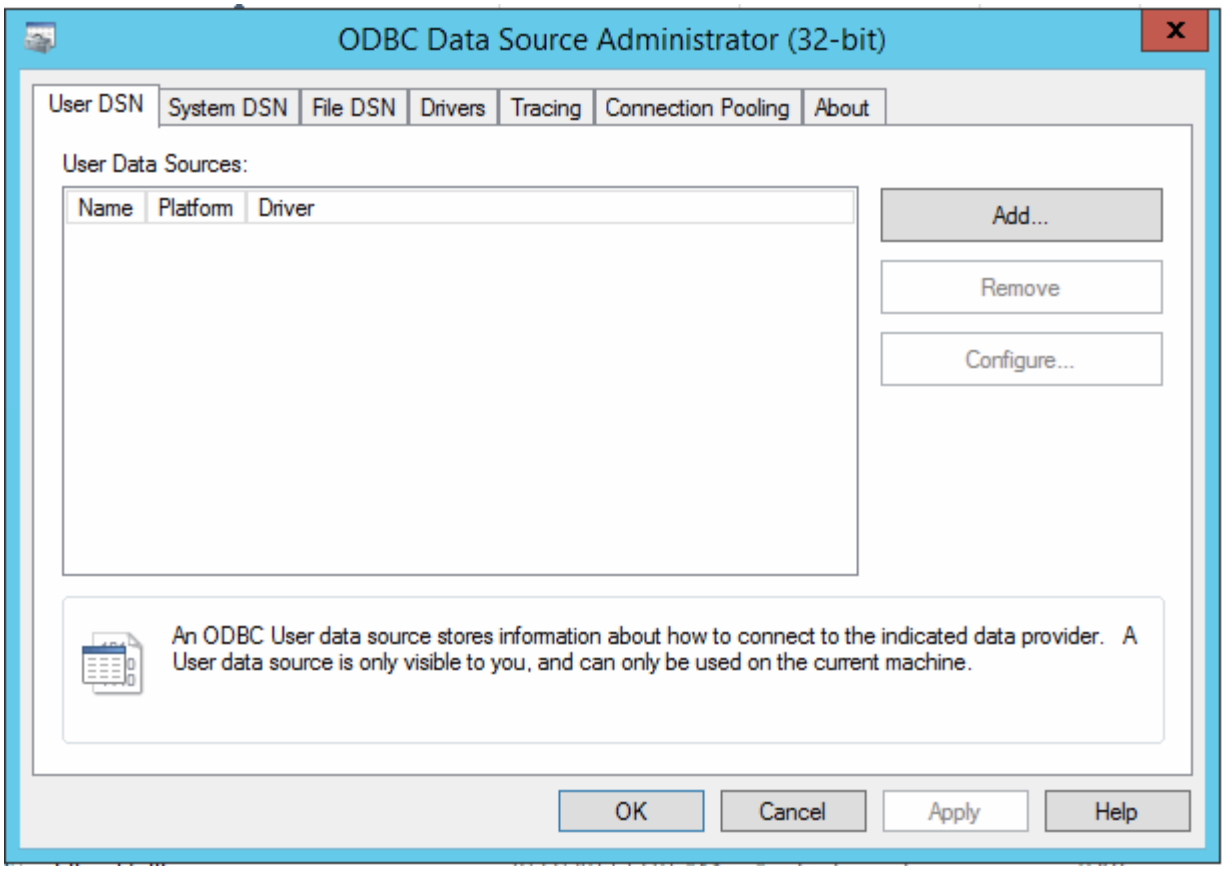
開始之前

您必須使用具有系統管理員權限的帳戶、遠端登入Data倉儲伺服器。

步驟

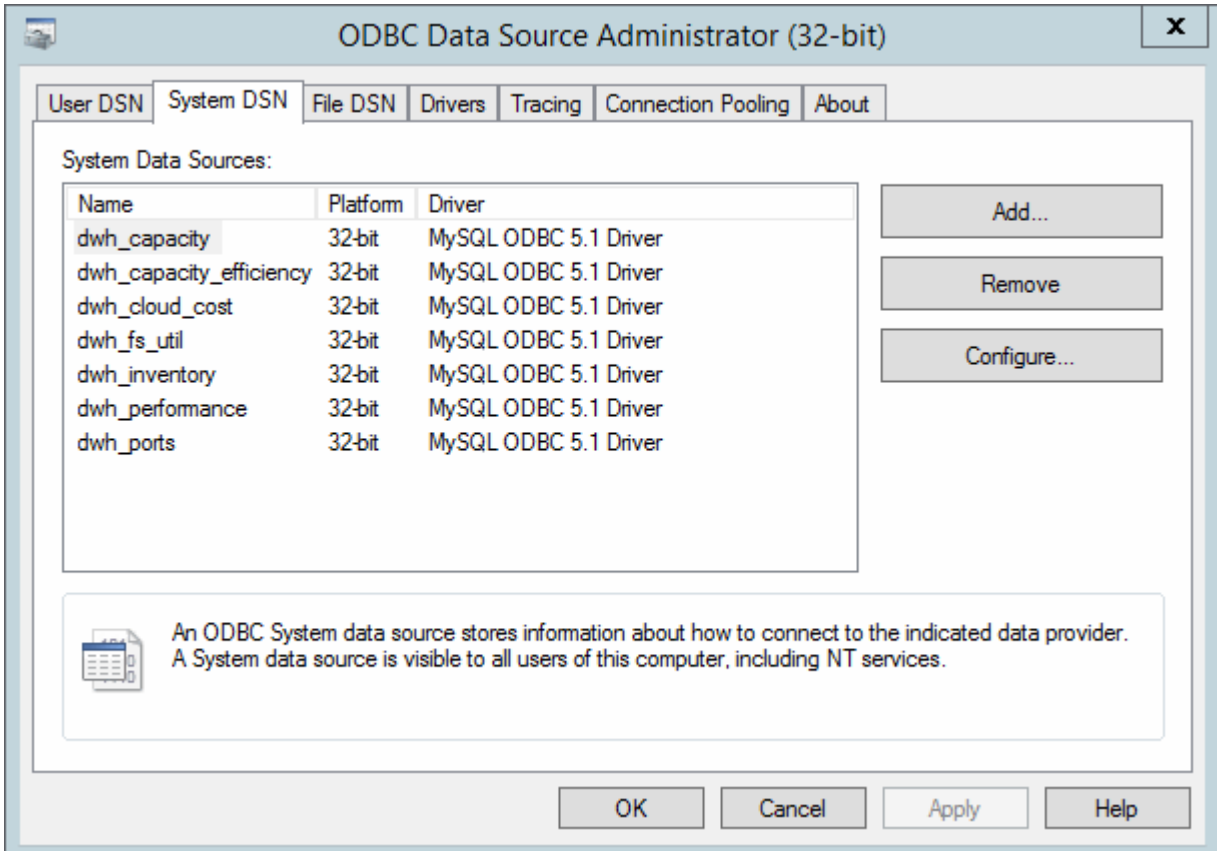
1. 遠端登入裝載該資料倉儲的伺服器。
2. 存取位於的「ODBC行政」工具 `C:\Windows\SysWOW64\odbcad32.exe`

   系統會顯示「ODBC資料來源管理員」畫面。



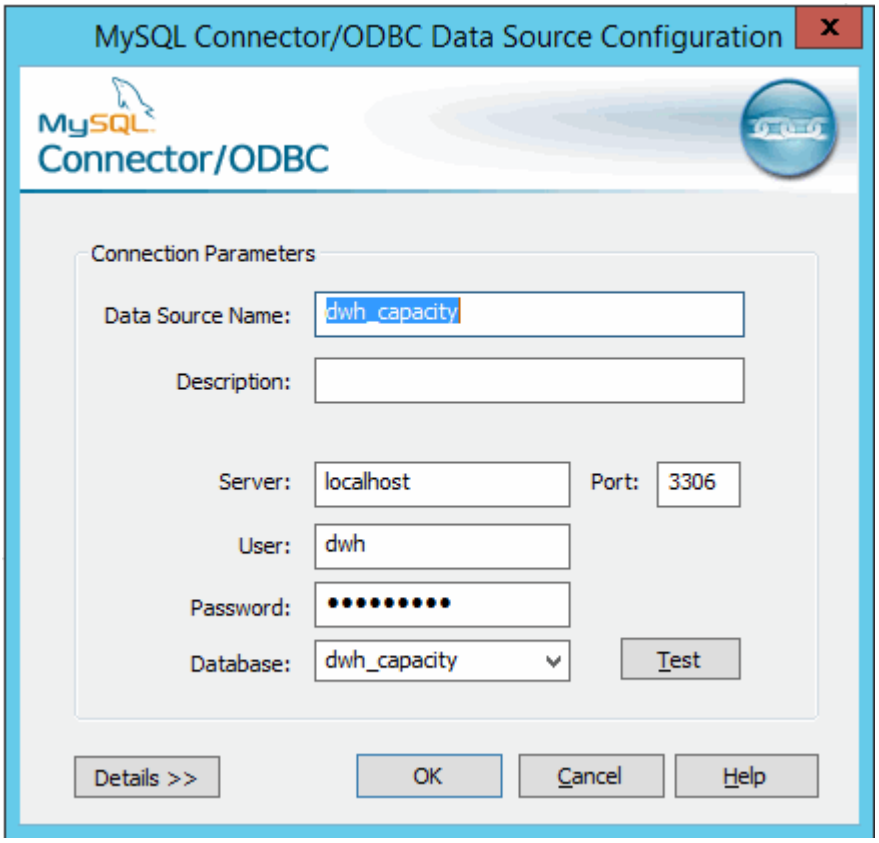
3. 單擊*系統DSN*

系統資料來源隨即顯示。



4. 從OnCommand Insight 清單中選取一個「支援資料來源」。
5. 按一下「設定」

   此時會顯示「Data來源組態」畫面。



6. 在*密碼*欄位中輸入新密碼。