Insight Security

OnCommand Insight

NetApp
April 01, 2024

目錄

Insight Security

7.3.1版OnCommand Insight 的功能介紹安全功能、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、以及變更加密和解密密碼的內部使用者密碼和金鑰配對的能力。您可以在Insight環境中的所有伺服器上管理這些功能。

Insight的預設安裝包括安全性組態、讓您環境中的所有站台共用相同的金鑰和相同的預設密碼。為了保護敏感資料、NetApp建議您在安裝或升級後變更預設金鑰和擷取使用者密碼。

資料來源加密密碼儲存在Insight Server資料庫中。伺服器具有公開金鑰、當使用者在WebUI資料來源組態頁面中輸入密碼時、會加密這些密碼。伺服器沒有解密儲存在伺服器資料庫中的資料來源密碼所需的私密金鑰。只有擷取單位（Lau、Rau）擁有解密資料來源密碼所需的資料來源私密金鑰。

重新輸入伺服器金鑰

使用預設金鑰會在您的環境中引進安全性弱點。根據預設、資料來源密碼會加密儲存在Insight資料庫中。加密時會使用所有Insight安裝通用的金鑰。在預設組態中、傳送至NetApp的Insight資料庫包含理論上可由NetApp解密的密碼。

變更擷取使用者密碼

使用預設的「擷取」使用者密碼會在您的環境中引入安全性弱點。所有擷取設備都會使用「擷取」使用者與伺服器通訊。使用預設密碼的Raus理論上可以使用預設密碼連線至任何Insight伺服器。

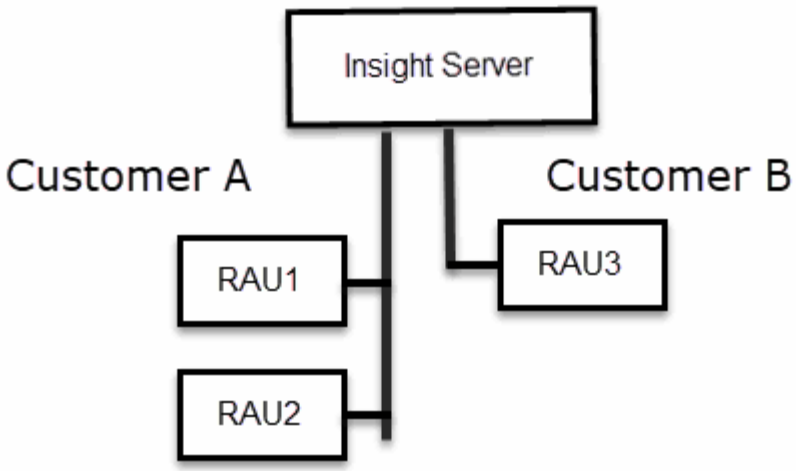
升級與安裝考量

如果Insight系統包含非預設的安全性組態（您已重新輸入或變更密碼）、則必須備份安全性組態。安裝新軟體、或在某些情況下升級軟體、會將系統還原為預設的安全組態。當系統恢復為預設組態時、您必須還原非預設組態、系統才能正常運作。

在複雜的服務供應商環境中管理金鑰

服務供應商可以託管OnCommand Insight 多個收集資料的客戶。這些金鑰可防止Insight伺服器上的多個客戶未經授權存取客戶資料。每位客戶的資料都受到其特定金鑰配對的保護。

Insight實作可設定如下圖所示。



您需要在此組態中為每位客戶建立個別的金鑰。客戶A需要兩個Raus相同的金鑰。客戶B需要一組金鑰。

您將採取哪些步驟來變更客戶A的加密金鑰：

1. 遠端登入裝載RAU1的伺服器。
2. 啟動安全性管理工具。
3. 選取變更加密金鑰以取代預設金鑰。
4. 選取備份以建立安全性組態的備份壓縮檔。
5. 遠端登入裝載RAU2的伺服器。
6. 將安全組態的備份壓縮檔複製到RAU2。
7. 啟動安全性管理工具。
8. 將安全備份從RAU1還原至目前的伺服器。

變更客戶B加密金鑰的步驟：

1. 遠端登入裝載RAU3的伺服器。
2. 啟動安全性管理工具。
3. 選取變更加密金鑰以取代預設金鑰。
4. 選取備份以建立安全性組態的備份壓縮檔。

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`

步驟

1. 遠端登入Insight伺服器。
2. 以互動模式啟動安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系統會要求登入認證資料。
3. 輸入具有「admin」認證的帳戶使用者名稱和密碼。
4. 選取*伺服器*。

   提供下列伺服器組態選項：

   - 備份

     建立包含所有密碼和金鑰的資料保險箱備份壓縮檔、並將檔案放置在使用者指定的位置、或是下列預設位置：

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

     還原所建立之資料保存庫的壓縮備份。還原之後、所有密碼和金鑰都會還原為建立備份時的現有值。

     > 還原可用於同步多個伺服器上的密碼和金鑰、例如：-變更單一伺服器上的伺服器加密金鑰-建立資料庫備份-將資料庫備份還原至第二個伺服器
   - 變更加密金鑰

     變更用來加密或解密Proxy使用者密碼、SMTP使用者密碼、LDAP使用者密碼等的伺服器加密金鑰。

     > 變更加密金鑰時、您應該備份新的安全性組態、以便在升級或安裝之後還原。
   - 更新密碼

     變更Insight使用的內部帳戶密碼。畫面會顯示下列選項：

     - 內部_

- 併購
- Cogns_admin
- dwh_internal
- 主機
- 庫存
- 根

> 有些帳戶需要在密碼變更時進行同步處理。例如、如果您變更伺服器上「擷取」使用者的密碼、則需要變更劉、Rau和DWH上「擷取」使用者的密碼以進行比對。此外、當您變更密碼時、也應該備份新的安全組態、以便在升級或安裝之後還原。

- 重設為預設值

  將金鑰和密碼重設為預設值。預設值為安裝期間提供的值。

- 退出

  結束 `securityadmin` 工具：

  a. 選擇您要變更的選項、然後依照提示進行。

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`

步驟

1. 遠端登入Insight伺服器。
2. 以互動模式啟動安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系統會要求登入認證資料。

3. 輸入具有「admin」認證的帳戶使用者名稱和密碼。
4. 選取*本機擷取單位*以重新設定本機擷取單位安全性組態。

   畫面會顯示下列選項：

   - 備份

     建立包含所有密碼和金鑰的資料保險箱備份壓縮檔、並將檔案放置在使用者指定的位置、或是下列預設位置：

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

   - 還原

     還原所建立之資料保存庫的壓縮備份。還原之後、所有密碼和金鑰都會還原為建立備份時的現有值。

     > 還原可用於同步多個伺服器上的密碼和金鑰、例如：-變更Lau上的加密金鑰-建立資料庫備份-將資料庫備份還原至每個Raus

   - 變更加密金鑰

     變更用於加密或解密裝置密碼的AU加密金鑰。

     > 變更加密金鑰時、您應該備份新的安全性組態、以便在升級或安裝之後還原。

   - 更新密碼

     變更「擷取」使用者帳戶的密碼。

     > 有些帳戶需要在密碼變更時進行同步處理。例如、如果您變更伺服器上「擷取」使用者的密碼、則需要變更劉、Rau和DWH上「擷取」使用者的密碼以進行比對。此外、當您變更密碼時、也應該備份新的安全組態、以便在升級或安裝之後還原。

   - 重設為預設值

     將擷取使用者密碼和擷取使用者加密金鑰重設為預設值、預設值為安裝期間提供的值。

   - 退出

     結束 `securityadmin` 工具：

5. 選擇您要設定的選項、然後依照提示進行。

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安全性組態的其中一種案例是、在伺服器上變更該使用者的密碼時、更新「擷取」使用者密碼。所有的Raus和Lau都使用與伺服器「擷取」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。

請使用下列步驟來管理Rau上的安全性選項：

步驟

1. 遠端登入執行Rau的伺服器
2. 以互動模式啟動安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系統會要求登入認證資料。
3. 輸入具有「admin」認證的帳戶使用者名稱和密碼。

   系統會顯示Rau功能表。

   - 備份

     建立包含所有密碼和金鑰的資料保險箱備份壓縮檔、並將檔案放置在使用者指定的位置、或是下列預設位置：

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

     還原所建立之資料保存庫的壓縮備份。還原之後、所有密碼和金鑰都會還原為建立備份時的現有值。

     > 還原可用於同步多個伺服器上的密碼和金鑰、例如：-變更一部伺服器上的加密金鑰-建立資料庫備份-將資料庫備份還原至第二部伺服器
   - 變更加密金鑰

     變更用來加密或解密裝置密碼的Rau加密金鑰。

     > 變更加密金鑰時、您應該備份新的安全性組態、以便在升級或安裝之後還原。
   - 更新密碼

變更「擷取」使用者帳戶的密碼。

> 有些帳戶需要在密碼變更時進行同步處理。例如、如果您變更伺服器上「擷取」使用者的密碼、則需要變更劉、Rau和DWH上「擷取」使用者的密碼以進行比對。此外、當您變更密碼時、也應該備份新的安全組態、以便在升級或安裝之後還原。

- 重設為預設值

  將加密金鑰和密碼重設為預設值。預設值為安裝期間提供的值。

- 退出

  結束 `securityadmin` 工具：

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`

步驟

1. 遠端登入資料倉儲伺服器。
2. 以互動模式啟動安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系統會要求登入認證資料。
3. 輸入具有「admin」認證的帳戶使用者名稱和密碼。

   系統會顯示資料倉儲的安全管理功能表：

   - 備份

     建立包含所有密碼和金鑰的資料保險箱備份壓縮檔、並將檔案放置在使用者指定的位置、或是預設位置：

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

- 還原

  還原所建立之資料保存庫的壓縮備份。還原之後、所有密碼和金鑰都會還原為建立備份時的現有值。

  > 還原可用於同步多個伺服器上的密碼和金鑰、例如：-變更一部伺服器上的加密金鑰-建立資料庫備份-將資料庫備份還原至第二部伺服器
  >
  > +

- 變更加密金鑰

  變更用於加密或解密密碼的DWH加密金鑰、例如連接器密碼和SMPT密碼。

- 更新密碼

  變更特定使用者帳戶的密碼。

  - 內部_
  - 併購
  - Cogns_admin
  - dwh
  - dwh_internal
  - dwhuser
  - 主機
  - 庫存
  - 根

  > 當您變更dwhuser、hosts、inventory或root密碼時、您可以選擇使用SHA-256密碼雜湊。此選項需要所有存取帳戶的用戶端都使用SSL連線。

+

- 重設為預設值

  將加密金鑰和密碼重設為預設值。預設值為安裝期間提供的值。

- 退出

  結束 `securityadmin` 工具：

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。

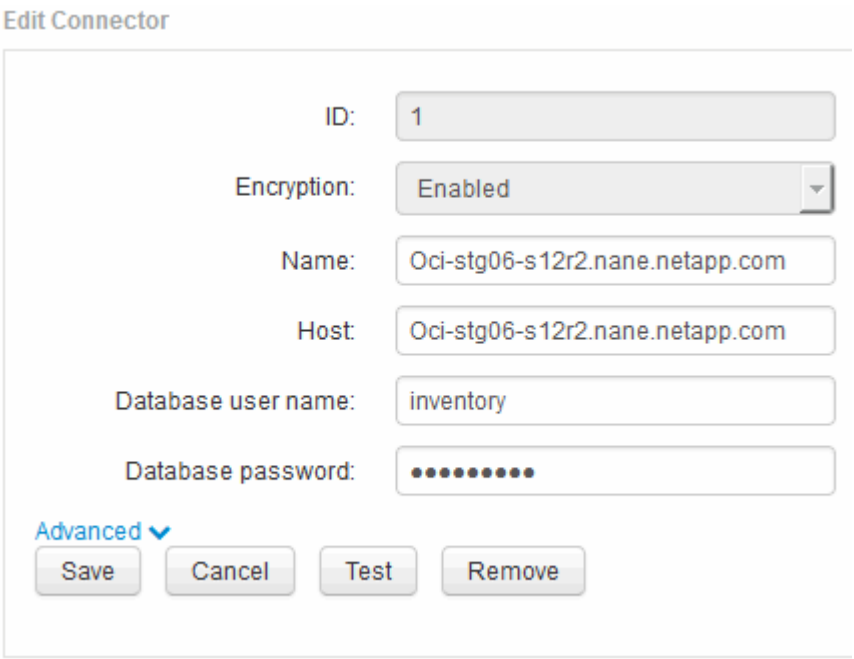
開始之前

您必須以系統管理員身分登入才能執行此工作。

步驟

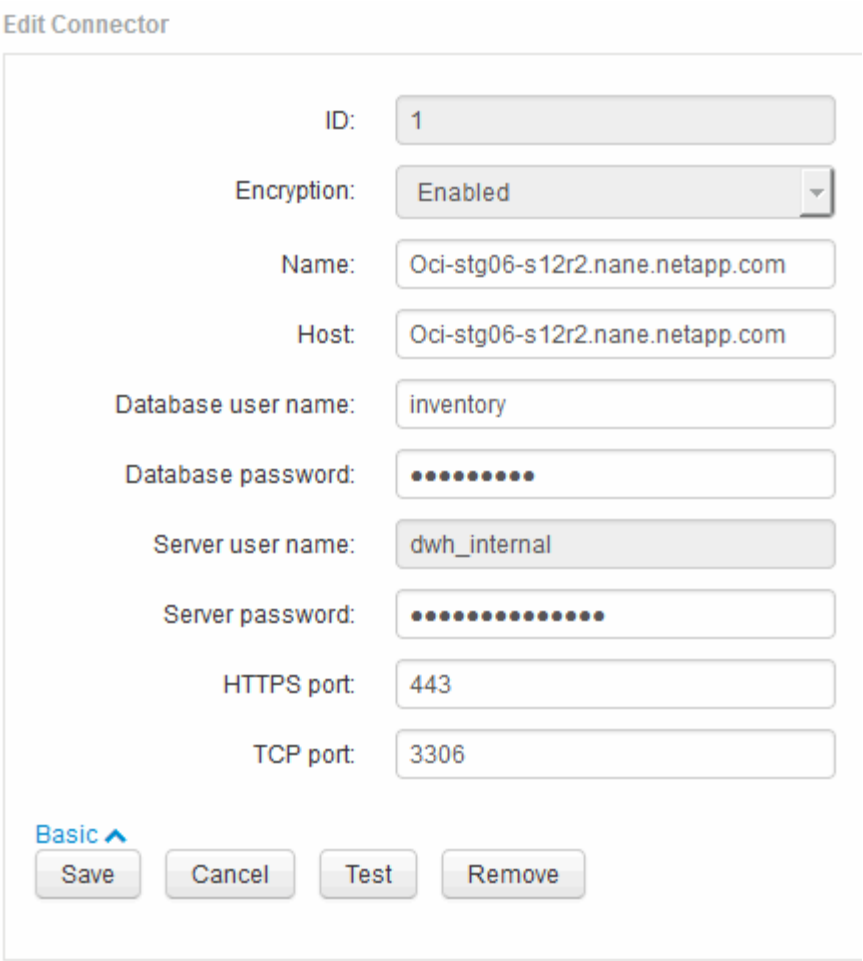
1. 登入資料倉儲入口網站： https://hostname/dwh、其中、主機名稱是OnCommand Insight 安裝了「IsorData倉儲」的系統名稱。
2. 在左側的導覽窗格中、按一下* Connectors *。

   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。

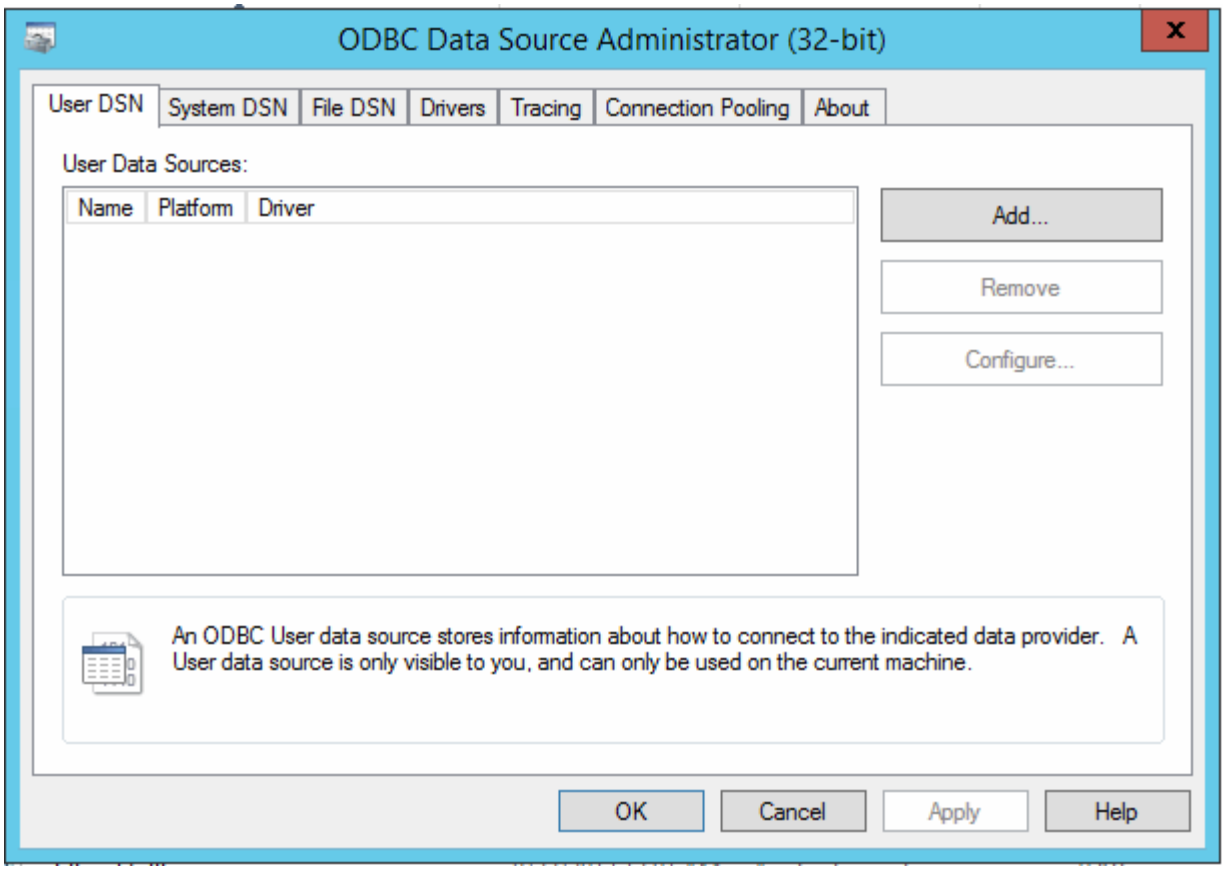
開始之前

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

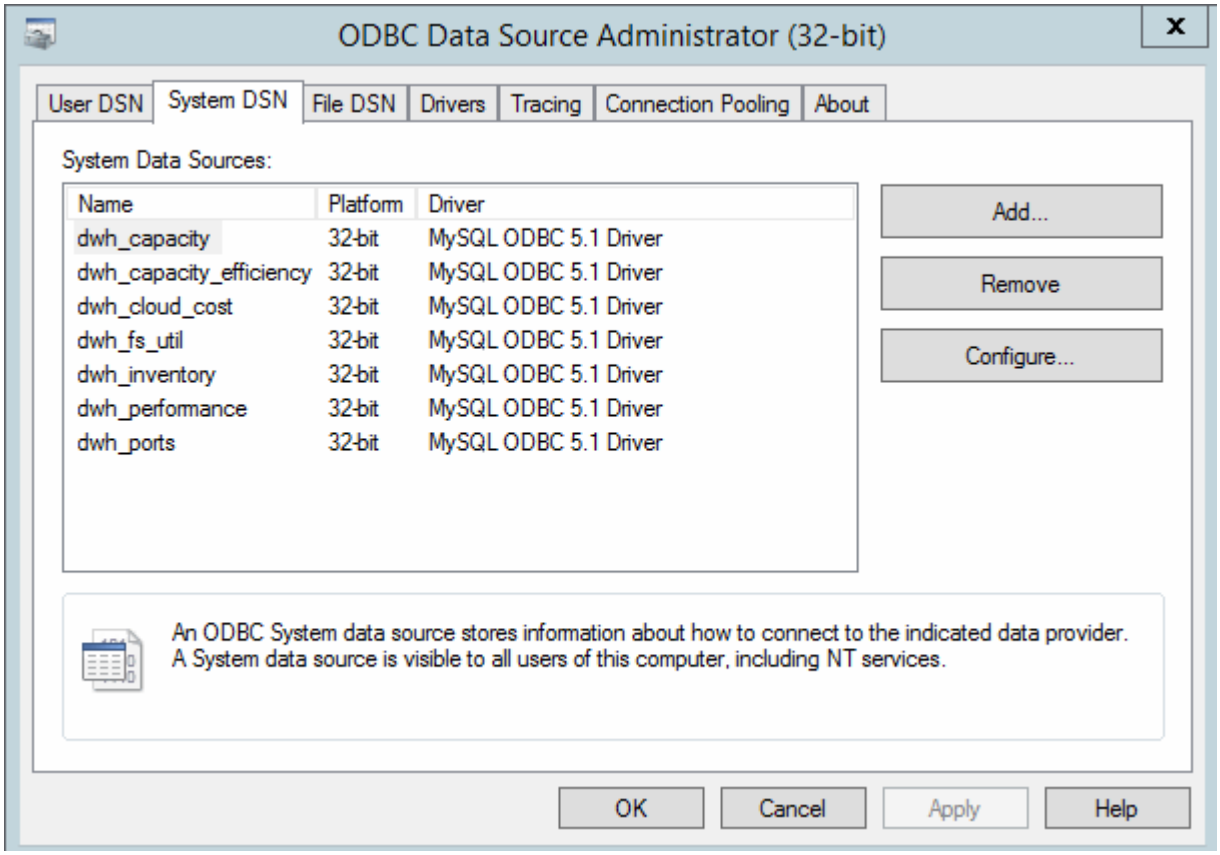
1. 遠端登入裝載該資料倉儲的伺服器。
2. 存取位於的「ODBC行政」工具 `C:\Windows\SysWOW64\odbcad32.exe`

   系統會顯示「ODBC資料來源管理員」畫面。



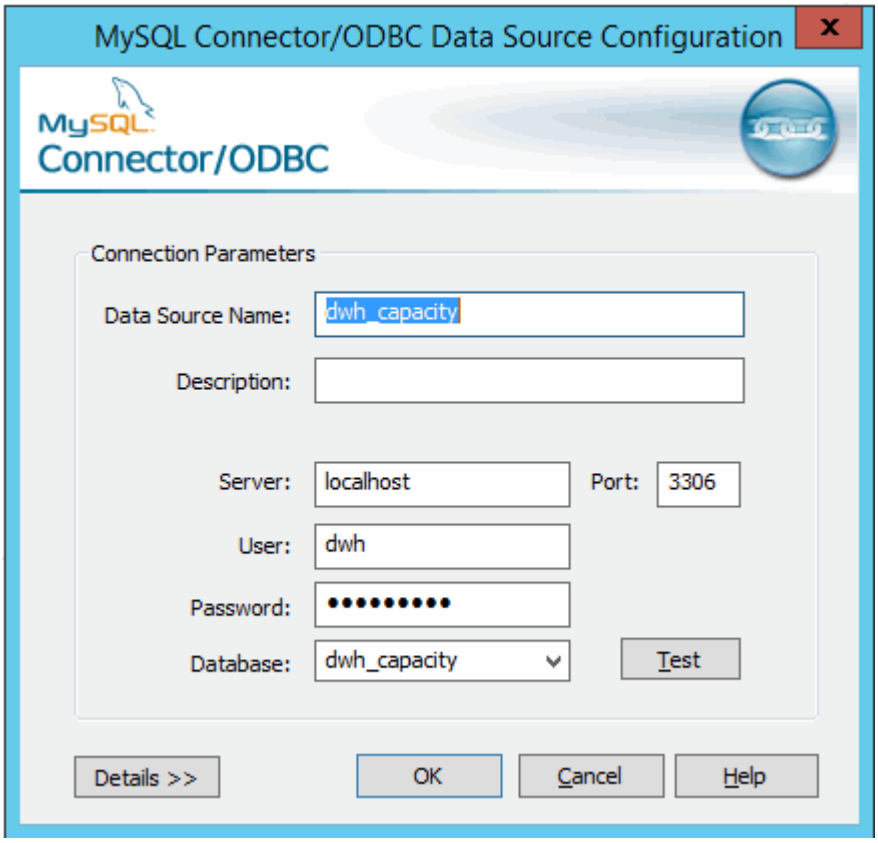
3. 單擊*系統DSN*

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。