Insight安全性

OnCommand Insight

NetApp
April 01, 2024

目录

Insight安全性

OnCommand Insight 7.3.1版引入了一些安全功能、可使Insight环境以增强的安全性运行。这些功能包括对加密、密码哈希以及更改内部用户密码和用于对密码进行加密和解密的密钥对的功能进行了改进。您可以在Insight环境中的所有服务器上管理这些功能。

Insight的默认安装包括一种安全配置、其中、环境中的所有站点共享相同的密钥和相同的默认密码。为了保护敏感数据、NetApp建议您在安装或升级后更改默认密钥和采集用户密码。

数据源加密密码存储在Insight Server数据库中。服务器具有一个公共密钥、当用户在WebUI数据源配置页面中输入密码时、它会对密码进行加密。服务器没有对存储在服务器数据库中的数据源密码进行解密所需的专用密钥。只有采集单元(LAU、RAU)具有解密数据源密码所需的数据源专用密钥。

重新设置服务器密钥

使用默认密钥会在您的环境中引入安全漏洞。默认情况下、数据源密码会以加密方式存储在Insight数据库中。它们使用所有Insight安装通用的密钥进行加密。在默认配置中、发送到NetApp的Insight数据库包含理论上可由NetApp解密的密码。

更改采集用户密码

使用默认的"采集"用户密码会在您的环境中引入安全漏洞。所有采集单元均使用"`Acquisition`"用户与服务器进行通信。理论上、使用默认密码的RAU可以使用默认密码连接到任何Insight服务器。

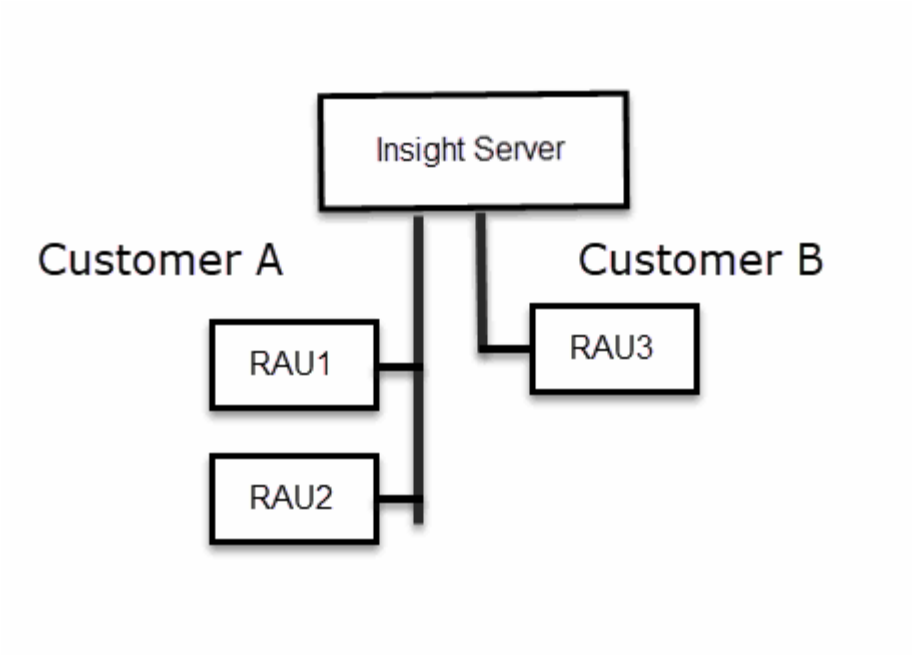
升级和安装注意事项

如果Insight系统包含非默认安全配置(您已重新设置密钥或更改密码)、则必须备份安全配置。安装新软件或在某些情况下升级软件会将系统还原为默认安全配置。当您的系统还原到默认配置时、您必须还原非默认配置、系统才能正常运行。

在复杂的服务提供商环境中管理密钥

一个服务提供商可以托管多个收集数据的OnCommand Insight 客户。这些密钥可防止多个客户在Insight服务器上未经授权访问客户数据。每个客户的数据都受其特定密钥对的保护。

可以按下图所示配置此Insight实施。



您需要为此配置中的每个客户创建单独的密钥。客户A要求两个RAU使用相同的密钥。客户B需要一组密钥。

更改客户A的加密密钥时应执行的步骤：

1. 远程登录到托管RAU1的服务器。
2. 启动安全管理工具。
3. 选择更改加密密钥以替换默认密钥。
4. 选择备份以创建安全配置的备份zip文件。
5. 远程登录到托管RAU2的服务器。
6. 将安全配置的备份zip文件复制到RAU2。
7. 启动安全管理工具。
8. 将安全备份从RAU1还原到当前服务器。

更改客户B的加密密钥时应执行的步骤：

1. 远程登录到托管RAU3的服务器。
2. 启动安全管理工具。
3. 选择更改加密密钥以替换默认密钥。
4. 选择备份以创建安全配置的备份zip文件。

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`

步骤

1. 远程登录到Insight服务器。
2. 在交互模式下启动安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系统请求登录凭据。
3. 输入具有"`Admin`"凭据的帐户的用户名和密码。
4. 选择 * 服务器 * 。

   可以使用以下服务器配置选项：

   - * 备份 *

     为包含所有密码和密钥的存储创建一个备份zip文件、并将该文件放置在用户指定的位置或以下默认位置：

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

     还原已创建的存储的zip备份。还原后、所有密码和密钥将还原为创建备份时的现有值。

     > 还原可用于同步多个服务器上的密码和密钥、例如：-更改一台服务器上的服务器加密密钥-创建存储的备份-将存储备份还原到第二台服务器
   - 更改加密密钥

     更改用于对代理用户密码、SMTP用户密码、LDAP用户密码等进行加密或解密的服务器加密密钥。

     > 更改加密密钥时、您应备份新的安全配置、以便在升级或安装后还原它。
   - 更新密码

     更改Insight使用的内部帐户的密码。此时将显示以下选项：

     - 内部
     - 采集

- Cognos_admin
- dwh_internal
- 主机
- 清单
- root

> 更改密码后、某些帐户需要同步。例如、如果您更改服务器上"采集"用户的密码、则需要更改LAU、RAU和DWH上"采集"用户的密码以使其匹配。此外、更改密码时、您应备份新的安全配置、以便在升级或安装后还原它。

- 重置为默认值

  将密钥和密码重置为默认值。默认值是在安装期间提供的值。

- * 退出 *

  退出 `securityadmin` 工具。

  a. 选择要更改的选项、然后按照提示进行操作。

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`

步骤

1. 远程登录到Insight服务器。
2. 在交互模式下启动安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系统请求登录凭据。

3. 输入具有"`Admin`"凭据的帐户的用户名和密码。
4. 选择*本地采集单元*以重新配置本地采集单元安全配置。

   此时将显示以下选项：

   - * 备份 *

     为包含所有密码和密钥的存储创建一个备份zip文件、并将该文件放置在用户指定的位置或以下默认位置：

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

   - * 还原 *

     还原已创建的存储的zip备份。还原后、所有密码和密钥将还原为创建备份时的现有值。

     > 还原可用于同步多个服务器上的密码和密钥、例如：-更改LAU上的加密密钥-创建存储备份-将存储备份还原到每个RAU

   - 更改加密密钥

     更改用于对设备密码进行加密或解密的AU加密密钥。

     > 更改加密密钥时、您应备份新的安全配置、以便在升级或安装后还原它。

   - 更新密码

     更改"采集"用户帐户的密码。

     > 更改密码后、某些帐户需要同步。例如、如果您更改服务器上"采集"用户的密码、则需要更改LAU、RAU和DWH上"采集"用户的密码以使其匹配。此外、更改密码时、您应备份新的安全配置、以便在升级或安装后还原它。

   - 重置为默认值

     将采集用户密码和采集用户加密密钥重置为默认值、默认值是在安装期间提供的值。

   - * 退出 *

     退出 `securityadmin` 工具。

5. 选择要配置的选项、然后按照提示进行操作。

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安全配置的一种情形是、在服务器上更改了"采集"用户密码后、RAU会更新该用户的密码。所有RAU和LAU都使用与服务器"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。

使用以下步骤管理RAU上的安全选项：

步骤

1. 远程登录到运行RAU的服务器
2. 在交互模式下启动安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系统请求登录凭据。
3. 输入具有"`Admin`"凭据的帐户的用户名和密码。

   系统将显示RAU的菜单。

   - * 备份 *

     为包含所有密码和密钥的存储创建一个备份zip文件、并将该文件放置在用户指定的位置或以下默认位置：

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

     还原已创建的存储的zip备份。还原后、所有密码和密钥将还原为创建备份时的现有值。

     > 还原可用于同步多个服务器上的密码和密钥、例如：-更改一个服务器上的加密密钥-创建存储备份-将存储备份还原到第二个服务器
   - 更改加密密钥

     更改用于对设备密码进行加密或解密的RAU加密密钥。

     > 更改加密密钥时、您应备份新的安全配置、以便在升级或安装后还原它。
   - 更新密码

更改"采集"用户帐户的密码。

> 更改密码后、某些帐户需要同步。例如、如果您更改服务器上"采集"用户的密码、则需要更改LAU、RAU和DWH上"采集"用户的密码以使其匹配。此外、更改密码时、您应备份新的安全配置、以便在升级或安装后还原它。

- 重置为默认值

  将加密密钥和密码重置为默认值。默认值是在安装期间提供的值。

- * 退出 *

  退出 `securityadmin` 工具。

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`

步骤

1. 远程登录到数据仓库服务器。
2. 在交互模式下启动安全管理工具：
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     系统请求登录凭据。
3. 输入具有"`Admin`"凭据的帐户的用户名和密码。

   系统将显示数据仓库的安全管理员菜单：

   - * 备份 *

     为包含所有密码和密钥的存储创建一个备份zip文件、并将该文件放置在用户指定的位置或默认位置：

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

还原已创建的存储的zip备份。还原后、所有密码和密钥将还原为创建备份时的现有值。

> 还原可用于同步多个服务器上的密码和密钥、例如：-更改一个服务器上的加密密钥-创建存储备份-将存储备份还原到第二个服务器
>
> +

- 更改加密密钥

  更改用于对连接器密码和SMPT密码等密码进行加密或解密的DWH加密密钥。

- 更新密码

  更改特定用户帐户的密码。

  - 内部
  - 采集
  - Cognos_admin
  - dwh
  - dwh_internal
  - dwhuser
  - 主机
  - 清单
  - root

> 更改dwhuser、hosts、inventory或root密码时、您可以选择使用SHA-256密码哈希。此选项要求访问这些帐户的所有客户端都使用SSL连接。

+

- 重置为默认值

  将加密密钥和密码重置为默认值。默认值是在安装期间提供的值。

- * 退出 *

  退出 `securityadmin` 工具。

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。

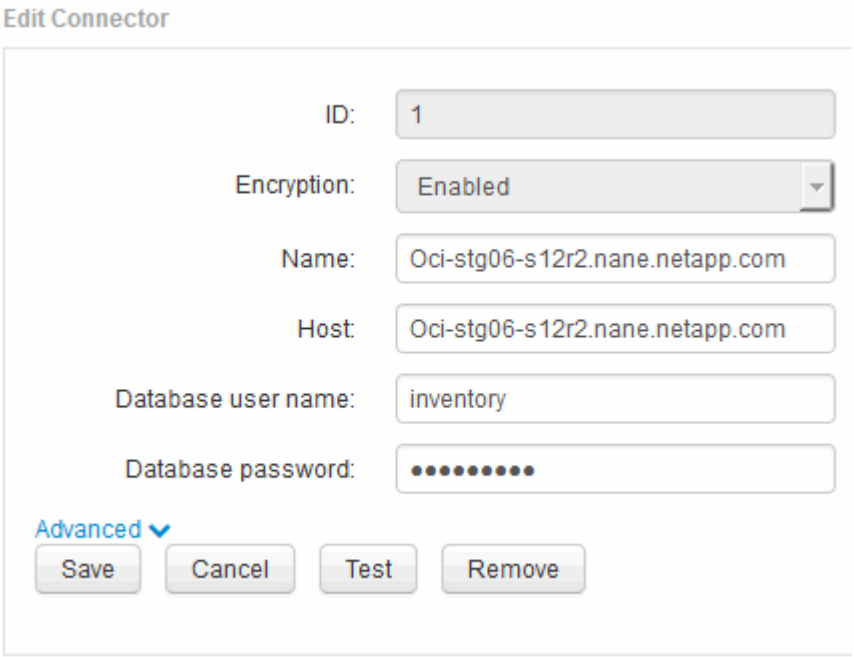
开始之前

要执行此任务、您必须以管理员身份登录。

步骤

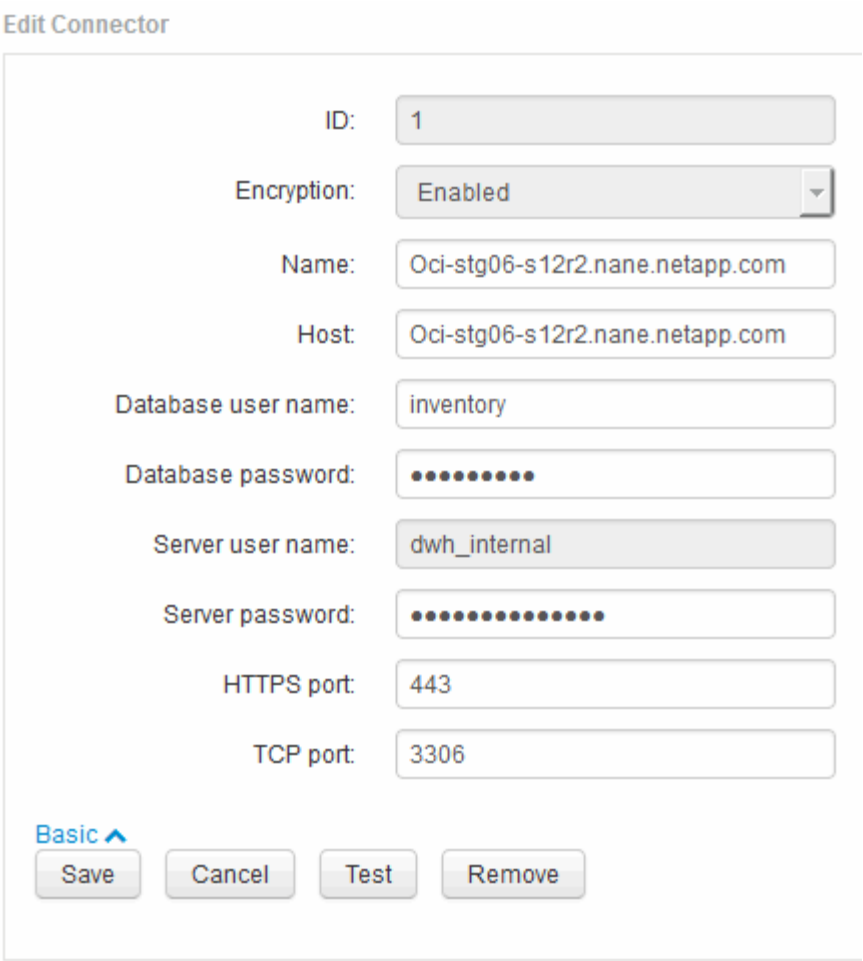
1. 登录到数据仓库门户、网址为 https://hostname/dwh、其中hostname是安装了OnCommand Insight 数据仓库的系统的名称。
2. 从左侧导航窗格中、单击*连接器*。

   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。

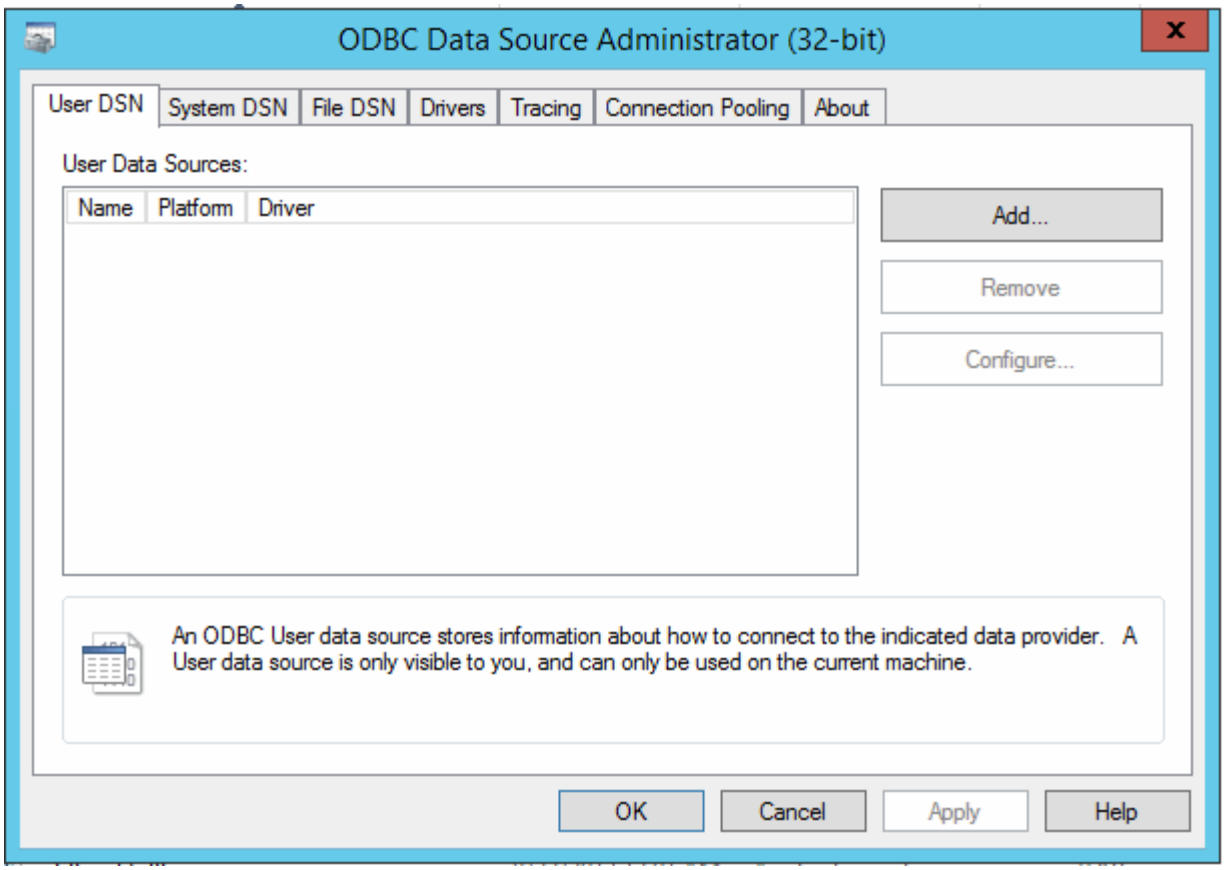
开始之前

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

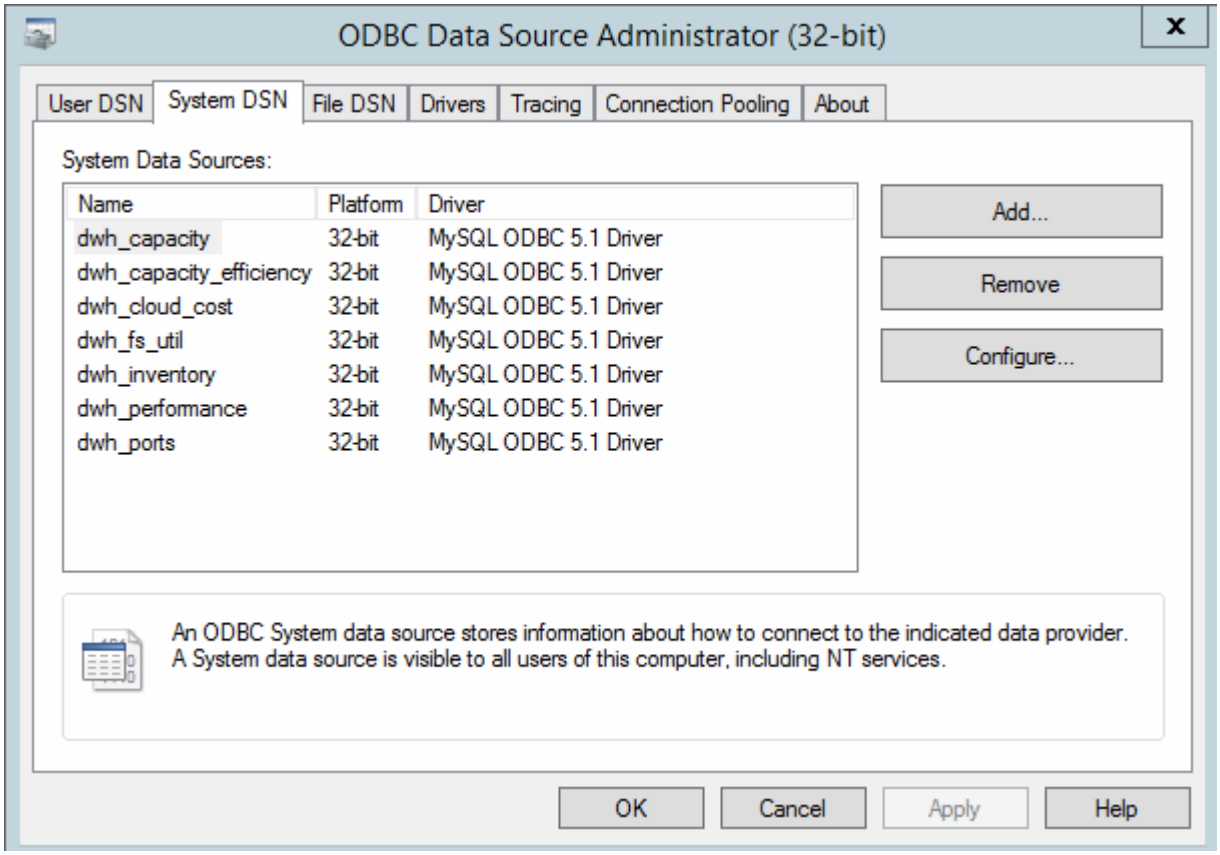
1. 远程登录到托管该数据仓库的服务器。
2. 访问ODBC管理工具、网址为 `C:\Windows\SysWOW64\odbcad32.exe`

   系统将显示"ODBC数据源管理员"屏幕。



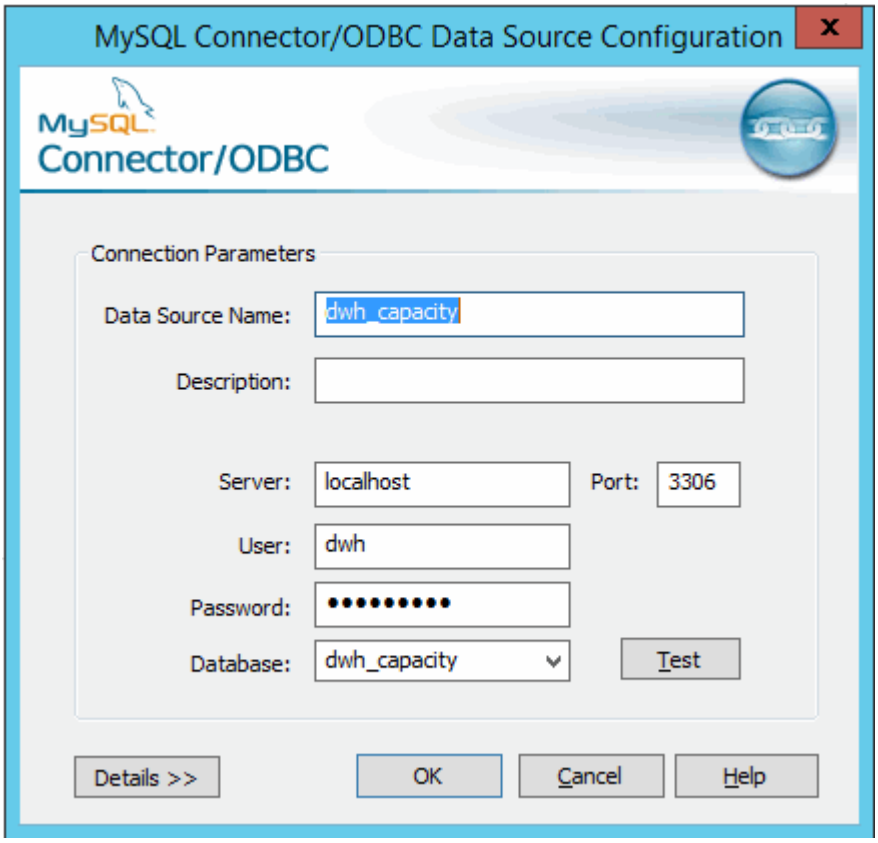
3. 单击*系统DSN*

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。