Insightセキュリティ

OnCommand Insight

NetApp
October 24, 2024

目次

Insightセキュリティ

OnCommand Insightには、Insight環境を高度なセキュリティで運用できる機能が用意されています。これらの機能には、暗号化、パスワードハッシュ、およびパスワードを暗号化および復号化する内部ユーザパスワードとキーペアを変更する機能が含まれます。これらの機能は、SecurityAdmin Toolを使用して、Insight環境内のすべてのサーバで管理できます。

SecurityAdminツールとは

セキュリティ管理ツールでは、ボルトの内容を変更したり、OnCommand Insightのインストール環境を調整したりすることができます。

SecurityAdminツールの主な用途は、セキュリティ設定（ボルトなど）およびパスワードの*バックアップ*および*リストア*です。たとえば、Local Acquisition Unitにバックアップを作成してRemote Acquisition Unitにリストアすることで、環境全体でパスワードの調整が可能になります。また、環境内に複数のOnCommand Insight Serverがある場合は、サーバーボルトのバックアップを作成し、パスワードを同じにするために他のサーバーに復元することもできます。これらは、SecurityAdminを使用して環境内で一貫性を確保する方法のほんの2つの例です。

OnCommand Insightデータベースをバックアップする場合は、必ず*ボルト*をバックアップすることを強くお勧めします。これを行わないと、アクセスが失われる可能性があります。

このツールには、*インタラクティブ*モードと*コマンドライン*モードの両方が用意されています。

SecurityAdmin Toolの多くの操作では、ボルトの内容が変更され、インストールも変更されます。これにより、ボルトとインストールの同期が維持されます。

例えば、

- ユーザのパスワードを変更すると、SANscreen .Usersテーブル内のユーザのエントリが新しいハッシュで更新されます。
- MySQLユーザーのパスワードを変更すると、適切なSQLステートメントが実行され、MySQLインスタンスのユーザーのパスワードが更新されます。

状況によっては、インストールに複数の変更が加えられることがあります。

- DWH MySQLユーザを変更すると、MySQLデータベースのパスワードが更新されるだけでなく、ODBCの複数のレジストリエントリも更新されます。

以降のセクションでは、これらの変更を「調整された変更」という用語で説明します。

実行モード

- 通常/デフォルト動作- SANscreenサーバサービスが実行されている必要があります

  デフォルトの実行モードでは、SecurityAdminツールは* SANscreenサーバーサービス*を実行している必要があります。サーバは認証に使用され、サーバを呼び出すことで、インストールに対する多くの調整さ

れた変更が行われます。

- 直接操作- SANscreenサーバサービスが実行中または停止している可能性があります。

  OCIサーバまたはDWHのインストール環境でツールを実行する場合は、「直接」モードでも実行できます。このモードでは、データベースを使用して認証と調整された変更が実行されます。Serverサービスは使用されません。

  動作は通常モードと同じですが、次の例外があります。

- ドメイン管理者以外のユーザに対してのみ認証がサポートされます。（パスワードとロールがLDAPではなくデータベースに存在するユーザ）。
- 「キーの置換」操作はサポートされていません。
- バックアップリストアの再暗号化手順はスキップされます。
- リカバリモードこのツールは、サーバーとデータベースの両方にアクセスできない場合でも実行できます（例えば、ボルト内のルートパスワードが正しくないため）。

  このモードで実行すると、認証ができないため、インストールに対して調整された変更を伴う操作は実行できません。

  リカバリモードは、次の目的で使用できます。

- どのボールトエントリが間違っているかを判断する（検証操作を使用）
- 間違ったrootパスワードを正しい値に置き換えます。（パスワードは変更されません。ユーザは現在のパスワードを入力する必要があります）。

> ボルト内のルートパスワードが正しくなく、パスワードが不明で、正しいルートパスワードを持つボルトのバックアップが存在しない場合、SecurityAdmin Toolを使用してインストールを復元することはできません。インストールを回復する唯一の方法は、に記載されている手順に従ってMySQLインスタンスのパスワードをリセットすることです https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html。リセット手順を実行した後、correct-stored-password操作を使用して新しいパスワードをボルトに入力します。

コマンド

制限されていないコマンド

無制限のコマンドは、インストールに対して調整された変更を行います（信頼ストアを除く）。制限のないコマンドは、ユーザ認証なしで実行できます。

コマンド	説明
バックアップ-ヴォールト	ボルトを含むzipファイルを作成します。ボールトファイルへの相対パスは、インストールルートを基準としたボールトパスと一致します。 • wildfly/standalone/configuration/vault/* • acq/conf/vault/*

check-for-default-keys	ボルトのキーが7.3.16より前のインスタンスで使用されていたデフォルトボルトのキーと一致するかどうかを確認します。
correct-stored-password	ボルトに保存されている（正しくない）パスワードを、ユーザーが知っている正しいパスワードに置き換えます。 これは、ボルトとインストールが一貫していない場合に使用できます。インストール時に実際のパスワードが変更されることはありません。
change-trust-store-password	信頼ストアに使用するパスワードを変更し、新しいパスワードをボルトに保存します。信頼ストアの現在のパスワードは「既知」である必要があります。
verify-keystore	ボルトの値が正しいかどうかを確認します。 • OCIユーザの場合、パスワードのハッシュがデータベース内の値と一致しているか • MySQLユーザの場合、データベースに接続できますか • キーストアの場合、キーストアをロードし、キー（存在する場合）を読み取ることができますか？
リストキー	ボルト内のエントリを一覧表示します（保存されている値は表示されません）。

制限されたコマンド

インストールに対して調整された変更を行う非表示のコマンドでは、認証が必要です。

コマンド	説明
restore-vault-backup	現在のボルトを、指定したボルトバックアップファイルに含まれているボルトで置き換えます。 すべての連携アクションを実行して、リストアされたボルトのパスワードと一致するようにインストールを更新します。 • OCI通信ユーザのパスワードを更新する • MySQLユーザのパスワード（rootを含む）を更新する • キーストアごとに、キーストアのパスワードが「既知」の場合は、復元されたボルトのパスワードを使用してキーストアを更新します。 通常モードで実行すると、はインスタンスから各暗号化された値を読み取り、現在のボールトの暗号化サービスを使用して復号化し、復元されたボールトの暗号化サービスを使用して再暗号化し、再暗号化された値を保存します。

synchronize-with-vault	すべての連携アクションを実行して、リストアされたボルトのユーザーパスワードと一致するようにインストールを更新します。 • OCI通信ユーザのパスワードを更新します。 • MySQLユーザのパスワード（rootを含む）を更新します。
パスワードの変更	ボルトのパスワードを変更し、調整された操作を実行します。
キーの置換	新しい空のボールト（既存のボールトとは異なるキーを持つ）を作成します。次に、現在のボルトから新しいボルトにエントリをコピーします。次に、インスタンスから各暗号化された値を読み取り、現在のボールトの暗号化サービスを使用して復号化し、復元されたボールトの暗号化サービスを使用して再暗号化し、再暗号化された値を保存します。

非表示コマンド

SAツールには次のコマンドが用意されています。これらのコマンドは認証を必要としませんが、インストールに対して調整された変更を行います。

リスト・キーのアップグレード（サーバ）	ユーザーが認証されていない場合は、現在のボルトで_internalアカウントとパスワードを使用して認証します。次に、現在のヴォールトをバックアップファイル内のヴォールトに置き換え、連携したアクションを実行します。
アップグレード（取得）	現在のボールトをバックアップファイル内のボールトに置き換え、調整されたアクションを実行します。

連携されたアクション

サーバーボールト

_internal	データベースのユーザのパスワードハッシュの更新
取得	データベースのユーザのパスワードハッシュの更新 取得ボールトが存在する場合は、取得ボールトのエントリも更新します。
dwh_internalの略	データベースのユーザのパスワードハッシュの更新
cognos_adminをクリックします	データベースのユーザのパスワードハッシュの更新 DWHおよびWindowsの場合は、SANscreen /cognos/analytics/configuration/SANscreenAP.propertiesを更新して、cognos.adminプロパティをパスワードに設定します。

ルート	SQLを実行してMySQLインスタンスのユーザパスワードを更新
在庫	SQLを実行してMySQLインスタンスのユーザパスワードを更新
DWH	SQLを実行してMySQLインスタンスのユーザパスワードを更新 DWHおよびWindowsの場合は、Windowsレジストリを更新して、次のODBC関連エントリを新しいパスワードに設定します。 • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_CAPACITY\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_CAPACITY_Efficiency\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_cost\pwd
誰だ	SQLを実行してMySQLインスタンスのユーザパスワードを更新
ホスト	SQLを実行してMySQLインスタンスのユーザパスワードを更新
キーストアパスワード	キーストアを新しいパスワード-wildfly/standalone/configuration/server.keystoreで書き換えます。
信頼ストアのパスワード	キーストアを新しいパスワード-wildfly/standalone/configuration/server.trustoreで書き換えます。
キーパスワード	キーストアを新しいパスワード-wildfly/standalone/configuration/sso.jksで書き換えます。

cognos_archive	なし

Acquisition Vault

取得	なし
信頼ストアのパスワード	キーストアを新しいパスワード（存在する場合）で書き換えます。 -acq/conf/cert/client.keystore

Security Adminツールの実行-コマンドライン

コマンドラインモードでSAツールを実行する構文は次のとおりです。

```
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：

- コマンドラインに「-i」オプションがない場合があります（対話モードが選択されるため）。
- 「-s」および「-au」オプションの場合：
  - 「-s」はRAUでは使用できません
  - DWHでは「-au」は使用できません
  - どちらも存在しない場合は、
    - サーバーボルトは、サーバー（Server）、DWH、およびデュアル（Dual）で選択されています。
    - RAUで収集ボールトが選択されている
- ユーザ認証には-luオプションと-lpオプションを使用します。
  - <user>が指定され、<password>が指定されていない場合は、ユーザにパスワードの入力を求められます。

◦ <user>を指定せず、認証が必要な場合は、<user>と<password>の両方の入力を求められます。

『コマンド・

コマンド	使用法
correct-stored-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 ` `	バックアップ-ヴォールト
`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 ` `
バックアップ-ヴォールト	`securityadmin [-s`

-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ```	リストキー
`` securityadmin [-s ```	-au] [-db] -l where -l specified command ```
チェックキー	``` securityadmin [-s ```
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ```	verify-keystore（サーバ）
`` securityadmin [-s] [-db] -v where -v specified command ```	アップグレード

`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 ``
キーの置換	`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（サーバ）	`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`

change - acquisitionユーザ（acquisition）のパスワード	`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.`
change-password for truststore -_password（acquisition）	`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.`
synchronize-with-vault（サーバー）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>` `where` `-sv specified command`

Security Admin Toolの実行-インタラクティブモード

インタラクティブ-メインメニュー

SAツールを対話型モードで実行するには、次のコマンドを入力します。

```
securityadmin -i
```

サーバまたはデュアルインストールの場合は、`SecurityAdmin`によってサーバまたは`Local Acquisition Unit`のどちらかを選択するように求められます。

ServerおよびAcquisition Unitノードが検出されました。セキュリティを再設定する必要があるノードを選択します。

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

DWHでは、[Server]が自動的に選択されます。リモートAUでは、「Acquisition Unit」が自動的に選択されます。

Interactive Server：rootパスワードのリカバリ

サーバーモードでは、SecurityAdminツールは最初に保存されているルートパスワードが正しいことを確認します。そうでない場合、ツールはrootパスワードの回復画面を表示します。

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

オプション1を選択すると、正しいパスワードの入力を求められます。

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

正しいパスワードを入力すると、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

間違ったパスワードを入力すると、次のメッセージが表示されます。

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

ENTERキーを押すと、リカバリメニューに戻ります。

オプション2を選択すると、正しいパスワードを読み取るバックアップファイルの名前の入力を求めるプロン

プトが表示されます。

```
 Enter Backup File Location:
```

バックアップのパスワードが正しい場合は、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

バックアップのパスワードが正しくない場合、次のメッセージが表示されます。

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

ENTERキーを押すと、リカバリメニューに戻ります。

Interactive-Server:正しいパスワード

「正しいパスワード」アクションは、ボルトに保存されているパスワードを変更し、インストールで必要とされる実際のパスワードと一致させるために使用されます。このコマンドは、securityadminツール以外によってインストールに変更が加えられた場合に便利です。たとえば、次のようなもの

- SQLユーザのパスワードがMySQLに直接アクセスして変更されました。
- キーストアが置き換えられたか、キーストアのパスワードがkeytoolを使用して変更されました。
- OCIデータベースがリストアされ、そのデータベースの内部ユーザ用に異なるパスワードが設定されている

「Correct Password」では、最初に正しい値を保存するパスワードを選択するように求められます。

```
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:
```

修正するエントリを選択すると、値の指定方法を求めるプロンプトが表示されます。

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

オプション1を選択すると、正しいパスワードの入力を求められます。

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

正しいパスワードを入力すると、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューに戻ります。

間違ったパスワードを入力すると、次のメッセージが表示されます。

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

ENTERキーを押すと、サーバーの無制限メニューに戻ります。

オプション2を選択すると、正しいパスワードを読み取るバックアップファイルの名前の入力を求めるプロンプトが表示されます。

```
 Enter Backup File Location:
```

バックアップのパスワードが正しい場合は、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

バックアップのパスワードが正しくない場合、次のメッセージが表示されます。

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

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

対話型サーバ：ボールトの内容の確認

ボルトの内容を確認（Verify Vault Contents）では、以前のバージョンのOCIで配布されたデフォルトのボルトと一致するキーがボルトにあるかどうかがチェックされ、ボルト内の各値がインストール環境と一致するかどうかがチェックされます。

各キーの結果は次のとおりです。

OK	ボルトの値が正しい

未チェック	この値はインストールに対してチェックできません
不良	値がインストール環境と一致しません
不明	想定されるエントリがありません。

```
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
```

対話型サーバ：バックアップ

Backupは、バックアップzipファイルを保存するディレクトリの入力を求めます。ディレクトリがすでに存在している必要があり、ファイル名はServerSecurityBackup-yyyy-mm-dd-hh-mm.zipになります。

```
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
```

対話型サーバ：ログイン

ログインアクションは、ユーザを認証し、インストールを変更する操作にアクセスするために使用されます。ユーザには管理Privilegesが必要です。サーバで実行する場合は、任意の管理者ユーザを使用できます。直接モードで実行する場合は、LDAPユーザではなくローカルユーザである必要があります。

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

または

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

UserName: admin

Password:
```

パスワードが正しく、ユーザが管理者ユーザである場合は、制限されたメニューが表示されます。

パスワードが正しくない場合は、次のメッセージが表示されます。

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

UserName: admin

Password:

Login Failed!
```

ユーザが管理者でない場合は、次のメッセージが表示されます。

```
Authenticating via server. Enter user and password

UserName: user

Password:

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

Interactive-Server:制限付きメニュー

ユーザーがログインすると、ツールに制限付きメニューが表示されます。

```
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:
```

Interactive-Server:パスワードの変更

「パスワードの変更」アクションは、インストールパスワードを新しい値に変更するために使用します。

[パスワードの変更]をクリックすると、最初に変更するパスワードを選択するように求められます。

```
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:
```

ユーザがMySQLユーザの場合、修正するエントリを選択すると、パスワードを強力にハッシュするかどうかを確認するメッセージが表示されます。

```
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
```

次に、新しいパスワードの入力を求められます。

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

Password is empty - cancelling operation
```

空でないパスワードを入力すると、パスワードの確認を求めるプロンプトが表示されます。

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

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

変更に失敗すると、エラーまたは例外が表示されます。

対話型サーバ：リストア

Interactive Server：暗号化キーの変更

暗号化キーの変更アクションは、ボールトエントリの暗号化に使用される暗号化キーを置き換え、ボールトの暗号化サービスに使用される暗号化キーを置き換えます。暗号化サービスのキーが変更されるため、データベース内の暗号化された値は再暗号化されます。これらの値は、現在のキーで読み取られ、復号化され、新しいキーで暗号化され、データベースに保存されます。

サーバは一部のデータベースコンテンツに対して再暗号化処理を提供するため、ダイレクトモードではこのアクションはサポートされていません。

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

Confirm (y/N): y

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

インタラクティブサーバー:インストールの修正

[インストールの修正]アクションを実行すると、インストールが更新されます。securityadminツールを使用して変更可能なすべてのインストールパスワード（rootを除く）は、ボルト内のパスワードに設定されます。

- OCIの内部ユーザのパスワードが更新されます。
- root以外のMySQLユーザのパスワードが更新されます。
- キーストアのパスワードが更新されます。

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

Confirm:  (y/N): y

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

最初の更新に失敗した時点でアクションが停止し、エラーまたは例外が表示されます。

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`

詳細については、のドキュメントを参照してください"securityadmin"。

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`

詳細については、手順を参照して"securityadminツール"ください。

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、サーバでその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。LAUおよびすべてのRAU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。

詳細については、手順を参照して"securityadminツール"ください。

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`

詳細については、のドキュメントを参照してください"securityadmin"。

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。

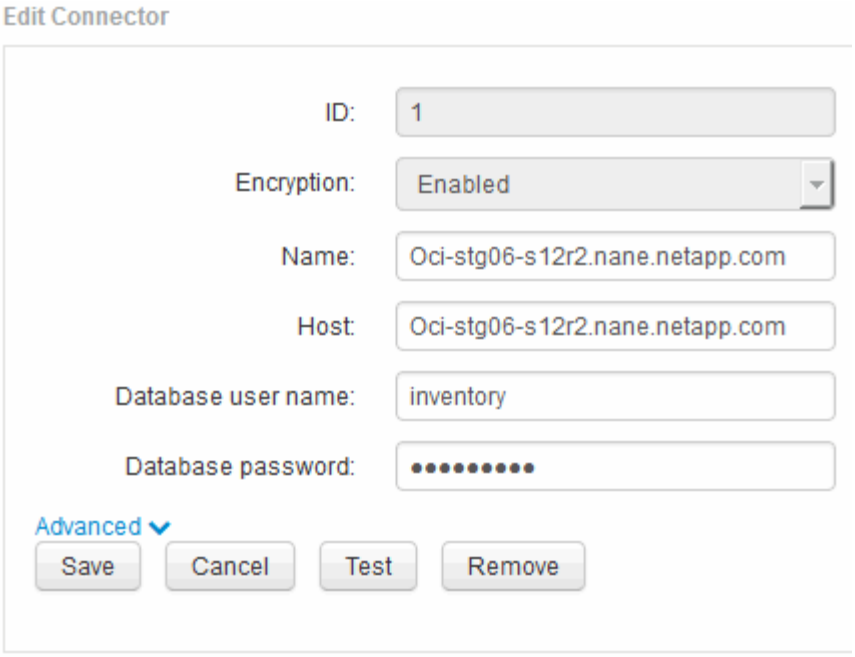
作業を開始する前に

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

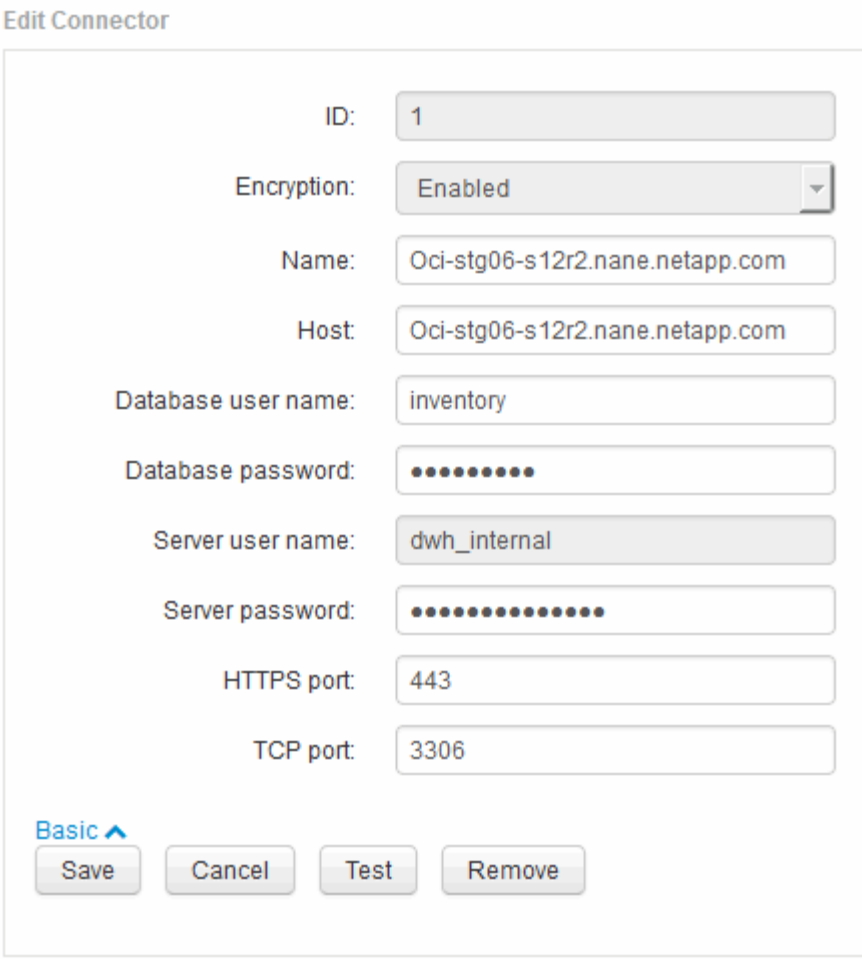
1. Data Warehouseポータルにログインします https://hostname/dwhhostnameは、OnCommand Insight Data Warehouseがインストールされているシステムの名前です。
2. 左側のナビゲーションペインで、*[コネクタ]*をクリックします。

   [Edit Connector]（コネクタの編集）*画面が表示されます。



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。



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。

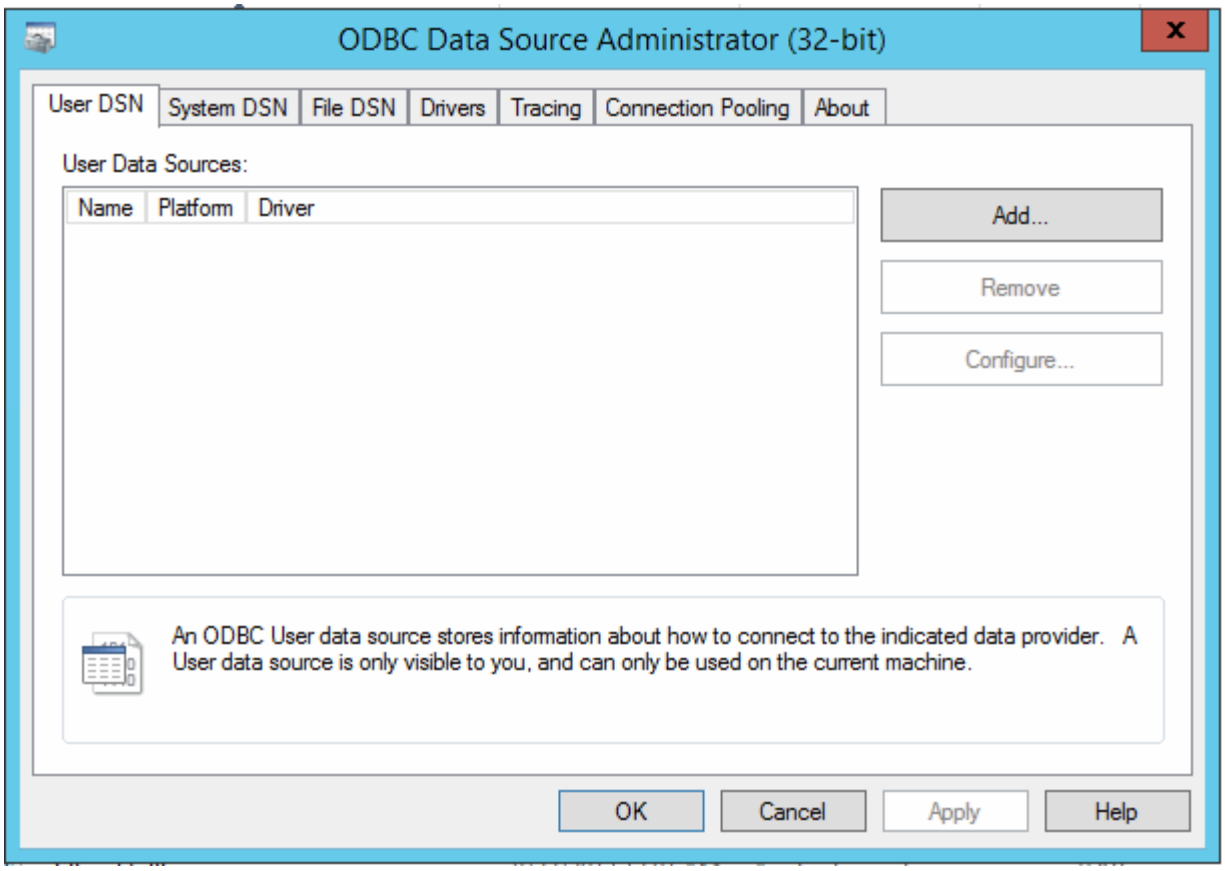
作業を開始する前に

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

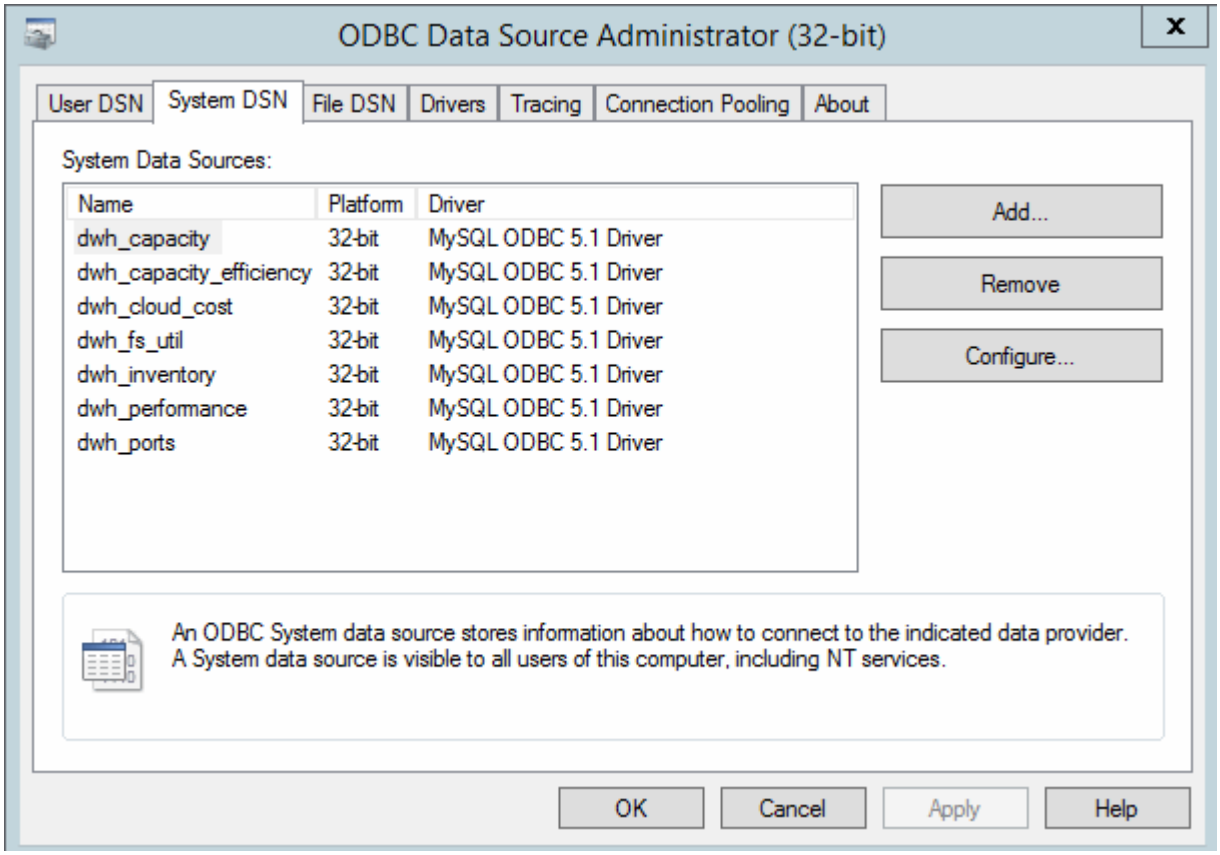
1. Data Warehouseをホストしているサーバへのリモートログインを実行します。
2. ODBC Administrationツールにアクセスします `C:\Windows\SysWOW64\odbcad32.exe`

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



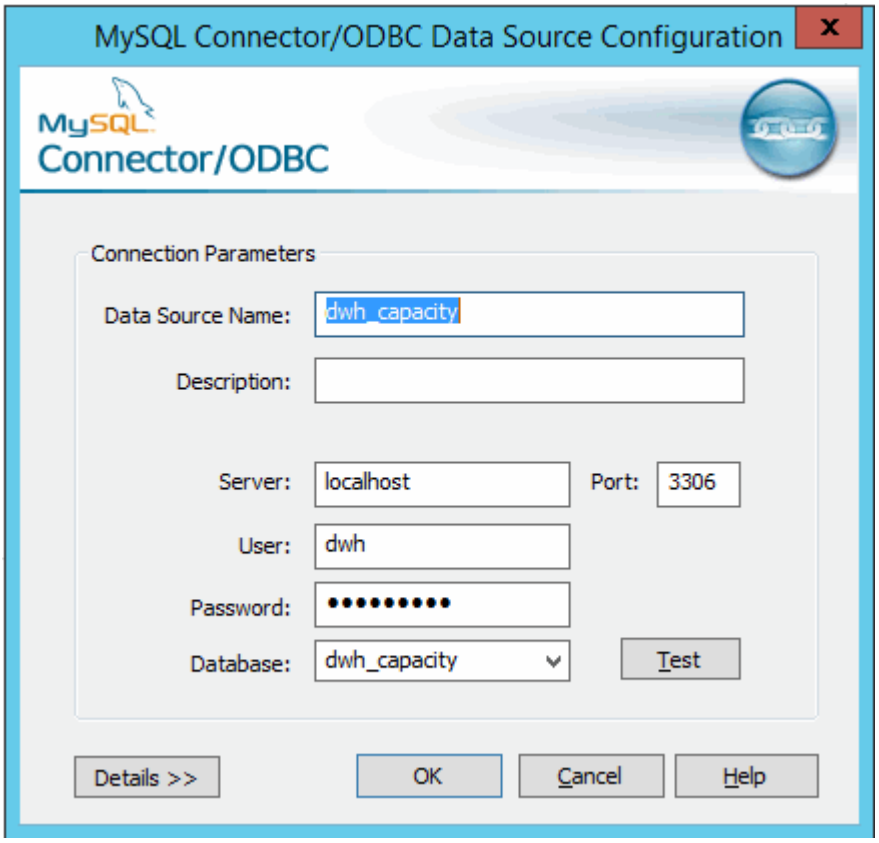
3. [システムDSN]*をクリックします

   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。



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

商標に関する情報