Insight 보안(SecurityAdmin 툴)

OnCommand Insight

NetApp
October 24, 2024

목차

SecurityAdmin 도구

OnCommand Insight은 Insight 환경을 향상된 보안으로 운영할 수 있도록 지원하는 기능을 제공합니다. 이러한 기능에는 암호화, 암호 해시, 내부 사용자 암호 및 암호를 암호화하고 해독하는 키 쌍을 변경하는 기능이 있습니다. SecurityAdmin Tool*을 사용하여 Insight 환경의 모든 서버에서 이러한 기능을 관리할 수 있습니다.

SecurityAdmin 도구란 무엇입니까?

보안 관리 도구는 볼트의 콘텐트를 변경하고 OnCommand Insight 설치에 대한 조정 변경을 지원합니다.

SecurityAdmin 도구의 주요 용도는 보안 구성(예: 볼트) 및 암호의 * 백업 * 및 * 복원 * 입니다. 예를 들어, 로컬 획득 장치에서 볼트를 백업하고 원격 획득 장치에서 복원할 수 있으므로 환경 전체에서 암호를 조정할 수 있습니다. 또는 사용자 환경에 OnCommand Insight 서버가 여러 개 있는 경우 서버 볼트를 백업한 후 다른 서버로 복원하여 암호를 동일하게 유지할 수 있습니다. SecurityAdmin을 사용하여 사용자 환경에서 결속력을 유지하는 방법의 두 가지 예에 불과합니다.

OnCommand Insight 데이터베이스를 백업할 때마다 * 볼트를 백업하는 것이 좋습니다 *. 그렇게 하지 않으면 액세스가 손실될 수 있습니다.

이 도구는 * 대화형 * 및 * 명령줄 * 모드를 모두 제공합니다.

많은 SecurityAdmin Tool 작업은 볼트의 내용을 변경하고 설치를 변경하여 볼트와 설치가 동기화된 상태로 유지되도록 합니다.

예를 들면, 다음과 같습니다.

- Insight 사용자 암호를 변경하면 SANscreen.users 테이블의 사용자 항목이 새 해시로 업데이트됩니다.
- MySQL 사용자의 암호를 변경하면 해당 SQL 문이 실행되어 MySQL 인스턴스에서 사용자의 암호를 업데이트합니다.

경우에 따라 설치가 여러 번 변경될 수 있습니다.

- dwh mysql 사용자를 수정하면 MySQL 데이터베이스의 암호를 업데이트하는 것 외에도 ODBC에 대한 여러 레지스트리 항목도 업데이트됩니다.

다음 섹션에서는 이러한 변경 사항을 설명하는 데 "조정된 변경"이라는 용어를 사용합니다.

실행 모드

- 일반/기본 작업 - SANscreen 서버 서비스가 실행 중이어야 합니다

  기본 실행 모드의 경우 SecurityAdmin 도구를 사용하려면 * SANscreen 서버 서비스 * 가 실행되고 있어야 합니다. 서버는 인증에 사용되며, 서버를 호출하여 설치에 대한 많은 조정 변경이 이루어집니다.

- 직접 작동 - SANscreen 서버 서비스가 실행 중이거나 중지되었을 수 있습니다.

  OCI 서버 또는 DWH 설치에서 실행되는 경우 도구는 "직접" 모드에서도 실행될 수 있습니다. 이 모드에서는

데이터베이스를 사용하여 인증 및 조정된 변경이 수행됩니다. 서버 서비스가 사용되지 않습니다.

다음과 같은 경우를 제외하고 정상 모드와 동일하게 작동합니다.

- 인증은 도메인 관리자가 아닌 사용자에게만 지원됩니다. (암호와 역할이 LDAP가 아닌 데이터베이스에 있는 사용자)
- "키 교체" 작업은 지원되지 않습니다.
- 볼트 복원의 재암호화 단계를 건너뜁니다.
- 복구 모드 이 도구는 서버와 데이터베이스 모두에 액세스할 수 없는 경우에도(예: 볼트의 루트 암호가 잘못되었기 때문에) 실행될 수 있습니다.

  이 모드에서 실행할 경우 인증이 불가능하며, 따라서 설치에 대한 조정 변경 작업이 수행되지 않을 수 있습니다.

  복구 모드는 다음과 같은 용도로 사용할 수 있습니다.

- 잘못된 볼트 항목을 확인합니다(확인 작업 사용).
- 잘못된 루트 암호를 올바른 값으로 교체합니다. (암호를 변경하지는 않습니다. 사용자는 현재 암호를 입력해야 합니다.)

> 볼트의 루트 암호가 올바르지 않고 암호를 알 수 없고 올바른 루트 암호를 가진 볼트 백업이 없는 경우 SecurityAdmin Tool을 사용하여 설치를 복구할 수 없습니다. 설치를 복구하는 유일한 방법은 에 설명된 절차에 따라 MySQL 인스턴스의 암호를 재설정하는 https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html 것입니다. 재설정 절차를 수행한 후 올바른 저장 암호 작업을 사용하여 볼트에 새 암호를 입력합니다.

명령

무제한 명령

무제한 명령은 설치에 대해 조정된 변경 사항을 적용합니다(신뢰 저장소 제외). 무제한 명령은 사용자 인증 없이 수행할 수 있습니다.

명령	설명
백업 볼트	볼트가 포함된 zip 파일을 작성합니다. 볼트 파일의 상대 경로는 설치 루트에 상대적인 볼트 경로와 일치합니다. • Wildfly/standalone/configuration/vault/ * • Acq/conf/볼트/ * OnCommand Insight 데이터베이스를 백업할 때마다 볼트를 백업하는 것이 좋습니다.
기본 키를 확인합니다	볼트의 키가 7.3.16 이전 인스턴스에 사용된 기본 볼트와 일치하는지 확인합니다.

올바른-저장된-암호	볼트에 저장된 (잘못된) 암호를 사용자가 알고 있는 올바른 암호로 바꿉니다. 볼트와 설치가 일치하지 않을 때 사용할 수 있습니다. 설치 시 실제 암호는 변경되지 않습니다.
	change-trust-store-password 트러스트 저장소에 사용되는 암호를 변경하고 볼트에 새 암호를 저장합니다. trust-store의 현재 암호는 "알려진" 암호여야 합니다.
verify-keystore 를 참조하십시오	볼트의 값이 올바른지 확인합니다. • OCI 사용자의 경우, 암호의 해시가 데이터베이스의 값과 일치합니까 • MySQL 사용자의 경우 데이터베이스 연결을 만들 수 있습니다 • 키 저장소의 경우 키 저장소를 로드하고 키(있는 경우)를 읽을 수 있습니다
목록 키	볼트에 있는 항목을 나열합니다(저장된 값을 표시하지 않음).

제한된 명령

숨겨지지 않은 모든 명령에 대한 인증이 필요하며, 이러한 명령은 설치에 대한 변경 사항을 조정합니다.

명령	설명
restore-vault-backup	현재 볼트를 지정된 볼트 백업 파일에 포함된 볼트로 대치합니다. 복원된 볼트의 암호와 일치하도록 설치를 업데이트하기 위해 조정된 모든 작업을 수행합니다. • OCI 통신 사용자 암호를 업데이트합니다 • root 를 포함하여 MySQL 사용자 암호를 업데이트합니다 • 각 키 저장소에 대해 키 저장소 암호가 "알려진" 경우 복원된 볼트의 암호를 사용하여 키 저장소를 업데이트합니다. 정상 모드에서 실행하면 는 인스턴스에서 암호화된 각 값을 읽고 현재 볼트의 암호화 서비스를 사용하여 암호를 해독하고 복원된 볼트의 암호화 서비스를 사용하여 다시 암호화한 다음 다시 암호화된 값을 저장합니다.
볼트와 동기화	복원된 볼트의 사용자 암호와 일치하도록 설치를 업데이트하기 위해 조정된 모든 작업을 수행합니다. • OCI 통신 사용자 암호를 업데이트합니다 • root 를 포함하여 MySQL 사용자 암호를 업데이트합니다
change-password(암호 변경	볼트의 암호를 변경하고 조정된 작업을 수행합니다.

교체 키	새 빈 볼트를 작성합니다(기존 볼트와 다른 키가 있음). 그런 다음 현재 볼트에서 새 볼트로 항목을 복사합니다. 그런 다음 인스턴스에서 암호화된 각 값을 읽고, 현재 볼트의 암호화 서비스를 사용하여 암호를 해독하고, 복원된 볼트의 암호화 서비스를 사용하여 다시 암호화한 후 다시 암호화된 값을 저장합니다.

조정된 작업

서버 볼트

_내부	데이터베이스의 사용자에 대한 암호 해시를 업데이트합니다
획득	데이터베이스의 사용자에 대한 암호 해시를 업데이트합니다 획득 볼트가 있으면 획득 볼트의 항목도 업데이트합니다
DWh _ 내부	데이터베이스의 사용자에 대한 암호 해시를 업데이트합니다
Cognos_admin	데이터베이스의 사용자에 대한 암호 해시를 업데이트합니다 DWH 및 Windows인 경우 SANscreen/cognos/analysis/configuration/SANscreenAP.properties 을 업데이트하여 cognos.admin 속성을 암호로 설정합니다.
루트	SQL을 실행하여 MySQL 인스턴스에서 사용자 암호를 업데이트합니다
인벤토리	SQL을 실행하여 MySQL 인스턴스에서 사용자 암호를 업데이트합니다

드Wh	SQL을 실행하여 MySQL 인스턴스에서 사용자 암호를 업데이트합니다 DWH 및 Windows의 경우 Windows 레지스트리를 업데이트하여 다음 ODBC 관련 항목을 새 암호로 설정합니다. • 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
Dwhuser(사용자)	SQL을 실행하여 MySQL 인스턴스에서 사용자 암호를 업데이트합니다
호스트	SQL을 실행하여 MySQL 인스턴스에서 사용자 암호를 업데이트합니다
keystore_password 를 입력합니다	새 암호(widdfly/standalone/configuration/server.keystore)를 사용하여 키 저장소를 다시 작성합니다
truststore_password입니다	새 암호(nandalone/configuration/server.trutstore)를 사용하여 키 저장소를 다시 작성합니다
KEY_PASSWORD	새 암호(widdfly/standalone/configuration/sso.jks)로 키 저장소를 다시 작성합니다
COGNOS_ARCHIVE 를 참조하십시오	없음

취득 볼트

획득	없음
truststore_password입니다	새 암호(있는 경우)로 키 저장소를 다시 작성합니다. acq/conf/cert/client.keystore

보안 관리 도구 실행 - 명령줄

명령줄 모드에서 SA 도구를 실행하는 구문은 다음과 같습니다.

```
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
```

참고:

- 명령줄에 "-i" 옵션이 표시되지 않을 수 있습니다(대화형 모드가 선택됨).
- "-s" 및 "-au" 옵션의 경우:
  - "-s"는 RAU에 허용되지 않습니다
  - DWH에서는 "-au"가 허용되지 않습니다
  - 둘 다 없는 경우
    - 서버 볼트가 서버, DWH, 이중에서 선택됩니다
    - RAU에서 획득 볼트가 선택됩니다
- 사용자 인증에 -lu 및 -lp 옵션이 사용됩니다.
  - <user>가 지정되고 <password>가 지정되지 않은 경우 사용자에게 암호를 묻는 메시지가 표시됩니다.
  - <user>가 제공되지 않고 인증이 필요한 경우 <user>와 <password>를 모두 입력하라는 메시지가 표시됩니다.

명령:

명령	사용
올바른-저장된-암호	`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 ` `	백업 볼트
`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 ` `
백업 볼트	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ` `	목록 키

`` securityadmin [-s ```	-au] [-db] -l where -l specified command ```
확인 키	``` securityadmin [-s ```
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ```	verify-keystore(서버)
`` securityadmin [-s] [-db] -v where -v specified command ```	업그레이드
`` 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 ```

교체 키	`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(서버)	`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 - 획득 사용자의 암호(획득)	`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(취득)	`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.`
볼트(서버)와 동기화	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>` `where` `-sv specified command`

보안 관리 도구 실행 - 대화형 모드

대화형 - 주 메뉴

대화형 모드에서 SA 도구를 실행하려면 다음 명령을 입력합니다.

```
 securityadmin -i
서버 또는 이중 설치에서 SecurityAdmin은 사용자에게 서버 또는 로컬 획득 장치를 선택하라는 메시지를 표시합니다.
```

서버 및 획득 장치 노드가 감지되었습니다! 보안을 다시 구성해야 하는 노드 선택:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

DWH에서 "서버"가 자동으로 선택됩니다. 원격 AU에서 "Acquisition Unit(획득 장치)"이 자동으로 선택됩니다.

Interactive-Server: 루트 암호 복구

서버 모드에서 SecurityAdmin Tool은 먼저 저장된 루트 암호가 올바른지 확인합니다. 그렇지 않으면 루트 암호 복구 화면이 표시됩니다.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

옵션 1을 선택하면 올바른 암호를 입력하라는 메시지가 표시됩니다.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
```
올바른 암호를 입력하면 다음이 표시됩니다.

```
 Password verified.  Vault updated
```
Enter 키를 누르면 서버 무제한 메뉴가 표시됩니다.

잘못된 암호를 입력하면 다음이 표시됩니다

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```
Enter 키를 누르면 복구 메뉴로 돌아갑니다.

옵션 2를 선택하면 올바른 암호를 읽을 백업 파일의 이름을 입력하라는 메시지가 표시됩니다.

```
 Enter Backup File Location:
```
백업의 암호가 올바르면 다음이 표시됩니다.

```
 Password verified.  Vault updated
```
Enter 키를 누르면 서버 무제한 메뉴가 표시됩니다.

백업의 암호가 올바르지 않으면 다음이 표시됩니다

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Enter 키를 누르면 복구 메뉴로 돌아갑니다.
```

Interactive-Server: 올바른 암호

"올바른 암호" 작업은 설치에 필요한 실제 암호와 일치하도록 볼트에 저장된 암호를 변경하는 데 사용됩니다. 이 명령은 SecurityAdmin 도구 이외의 다른 방법으로 설치를 변경한 경우에 유용합니다. 예를 들면 다음과 같습니다.

- SQL 사용자의 암호가 MySQL에 직접 액세스하여 수정되었습니다.
- 키 저장소를 교체하거나 키 도구를 사용하여 키 저장소의 암호를 변경합니다.
- OCI 데이터베이스가 복원되었고 해당 데이터베이스의 내부 사용자에 대해 서로 다른 암호가 있습니다

"암호 수정"은 먼저 사용자에게 올바른 값을 저장할 암호를 선택하라는 메시지를 표시합니다.

```
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:
```

수정할 항목을 선택하면 사용자가 값을 제공할 방법을 묻는 메시지가 표시됩니다.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

옵션 1을 선택하면 올바른 암호를 입력하라는 메시지가 표시됩니다.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
```
올바른 암호를 입력하면 다음이 표시됩니다.

```
 Password verified.  Vault updated
Enter 키를 누르면 서버 무제한 메뉴로 돌아갑니다.
```

잘못된 암호를 입력하면 다음이 표시됩니다

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

Enter 키를 누르면 서버 무제한 메뉴로 돌아갑니다.

옵션 2를 선택하면 올바른 암호를 읽을 백업 파일의 이름을 입력하라는 메시지가 표시됩니다.

```
 Enter Backup File Location:
```
백업의 암호가 올바르면 다음이 표시됩니다.

```
 Password verified.  Vault updated
Enter 키를 누르면 서버 무제한 메뉴가 표시됩니다.
```

백업의 암호가 올바르지 않으면 다음이 표시됩니다

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

Enter 키를 누르면 서버 무제한 메뉴가 표시됩니다.

Interactive-Server: 볼트 내용 확인

볼트 콘텐트가 볼트에 이전 OCI 버전과 배포된 기본 볼트와 일치하는 키가 있는지 확인하고 볼트의 각 값이 설치와 일치하는지 확인합니다.

각 키에 대해 가능한 결과는 다음과 같습니다.

좋습니다	볼트 값이 올바릅니다
선택되지 않았습니다	값을 설치에 대해 확인할 수 없습니다

나쁘다	값이 설치와 일치하지 않습니다
없습니다	필요한 항목이 누락되었습니다.

```
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
```

대화형 서버: 백업

백업 zip 파일을 저장할 디렉토리를 묻는 메시지가 표시됩니다. 디렉터리가 이미 존재해야 하며 파일 이름은 ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip이 됩니다.

```
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
```

대화형 - 서버: 로그인

로그인 작업은 사용자를 인증하고 설치를 수정하는 작업에 대한 액세스 권한을 얻는 데 사용됩니다. 사용자에게 admin Privileges가 있어야 합니다. 서버에서 실행하는 경우 모든 관리자 사용자를 사용할 수 있습니다. 직접 모드에서 실행하는 경우 사용자는 LDAP 사용자가 아닌 로컬 사용자여야 합니다.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

또는

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

UserName: admin

Password:
```

암호가 올바르고 사용자가 관리자 사용자인 경우 제한된 메뉴가 표시됩니다.

암호가 올바르지 않으면 다음과 같은 메시지가 표시됩니다.

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

UserName: admin

Password:

Login Failed!
```

사용자가 관리자가 아닌 경우 다음이 표시됩니다.

```
Authenticating via server. Enter user and password

UserName: user

Password:

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

대화형 서버: 제한된 메뉴

사용자가 로그인하면 도구에 제한된 메뉴가 표시됩니다.

```
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: 암호 변경

"암호 변경" 작업은 설치 암호를 새 값으로 변경하는 데 사용됩니다.

"암호 변경"은 먼저 변경할 암호를 선택하라는 메시지를 사용자에게 표시합니다.

```
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:
```

수정할 항목을 선택한 후 사용자가 MySQL 사용자인 경우 암호에 대한 강력한 해시를 수행할지 묻는 메시지가 표시됩니다

```
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
```

그런 다음 새 암호를 입력하라는 메시지가 표시됩니다.

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

Password is empty - cancelling operation
```

비어 있지 않은 암호를 입력하면 암호를 확인하라는 메시지가 표시됩니다.

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

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

변경에 실패하면 오류 또는 예외가 표시됩니다.

대화형 서버: 복원

Interactive-Server: 암호화 키 변경

암호화 키 변경 작업은 볼트 항목을 암호화하는 데 사용되는 암호화 키를 대체하고 볼트의 암호화 서비스에 사용된 암호화 키를 대체합니다. 암호화 서비스의 키가 변경되기 때문에 데이터베이스에서 암호화된 값은 다시 암호화됩니다. 즉, 이 값은 읽혀지고 현재 키로 해독되며 새 키로 암호화되어 데이터베이스에 다시 저장됩니다.

서버가 일부 데이터베이스 콘텐츠에 대해 다시 암호화 작업을 제공하므로 이 작업은 직접 모드에서는 지원되지 않습니다.

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

Confirm (y/N): y

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

Interactive-Server: 설치 수정

설치 수정 작업을 수행하면 설치가 업데이트됩니다. SecurityAdmin 도구를 통해 변경할 수 있는 모든 설치 암호(root 제외)는 볼트의 암호로 설정됩니다.

- OCI 내부 사용자의 암호가 업데이트됩니다.
- root 를 제외한 MySQL 사용자의 암호가 업데이트됩니다.
- 키 저장소의 암호가 업데이트됩니다.

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

Confirm:  (y/N): y

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

첫 번째 업데이트 실패 시 작업이 중지되고 오류 또는 예외가 표시됩니다.

Insight 서버의 보안 관리

를 클릭합니다 `securityadmin` 도구를 사용하면 Insight 서버의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 암호 변경, 새 키 생성, 사용자가 만든 보안 구성 저장 및 복원, 기본 설정으로 구성 복원 등이 포함됩니다.

이 작업에 대해

를 사용합니다 `securityadmin` 보안 관리 도구:

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

"SecurityAdmin 을 클릭합니다"자세한 내용은 설명서를 참조하십시오.

로컬 획득 장치의 보안 관리

를 클릭합니다 `securityadmin` 도구를 사용하면 로컬 획득 사용자(Lau)의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 키 및 암호 관리, 사용자가 만들고 복원한 보안 구성을 기본 설정으로 저장 및 복원하는 작업이 포함됩니다.

시작하기 전에

이(가) 있어야 합니다 `admin` 보안 구성 작업을 수행할 수 있는 권한.

이 작업에 대해

를 사용합니다 `securityadmin` 보안 관리 도구:

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

자세한 내용은 지침을 "SecurityAdmin 도구"참조하십시오.

RAU에 대한 보안 관리

를 클릭합니다 `securityadmin` 도구를 사용하면 RA의 보안 옵션을 관리할 수 있습니다. 볼트 구성을 백업 또는 복원하거나 암호화 키를 변경하거나 획득 장치의 암호를 업데이트해야 할 수 있습니다.

이 작업에 대해

를 사용합니다 `securityadmin` 보안 관리 도구:

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

LAU/RAU에 대한 보안 구성을 업데이트하는 한 가지 시나리오는 서버에서 해당 사용자의 암호가 변경될 때 '획득' 사용자 암호를 업데이트하는 것입니다. LAU 및 모든 RAU는 서버와 통신하기 위해 서버 '취득' 사용자의 암호와 동일한 암호를 사용합니다.

'acquisition' 사용자는 Insight 서버에만 있습니다. RAU 또는 Lau는 서버에 연결할 때 해당 사용자로 로그인합니다.

자세한 내용은 지침을 "SecurityAdmin 도구"참조하십시오.

데이터 웨어하우스의 보안 관리

를 클릭합니다 `securityadmin` 도구를 사용하면 데이터 웨어하우스 서버의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 DWH 서버의 내부 사용자에 대한 내부 암호 업데이트, 보안 구성 백업 생성 또는 기본 설정으로 구성 복원이 포함됩니다.

이 작업에 대해

를 사용합니다 `securityadmin` 보안 관리 도구:

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

"SecurityAdmin 을 클릭합니다"자세한 내용은 설명서를 참조하십시오.

OnCommand Insight 내부 사용자 암호 변경

보안 정책에 따라 OnCommand Insight 환경의 암호를 변경해야 할 수 있습니다. 한 서버의 암호 중 일부는 환경의 다른 서버에 있으므로 두 서버의 암호를 변경해야 합니다. 예를 들어, Insight Server에서 ""인벤토리"" 사용자 암호를 변경할 경우 해당 Insight Server에 대해 구성된 데이터 웨어하우스 서버 Connector의 ""인벤토리"" 사용자 암호와 일치해야 합니다.

시작하기 전에

암호를 변경하기 전에 사용자 계정의 종속성을 이해해야 합니다. 필요한 모든 서버에서 암호를 업데이트하지 못하면 Insight 구성 요소 간의 통신 장애가 발생합니다.

이 작업에 대해

다음 표에는 Insight Server의 내부 사용자 암호가 나열되어 있으며 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

Insight Server 암호	필수 변경 사항
_내부	
획득	Lau, RAU
DWh _ 내부	데이터 웨어하우스
호스트	
인벤토리	데이터 웨어하우스
루트	

다음 표에는 데이터 웨어하우스에 대한 내부 사용자 암호가 나열되어 있으며 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

데이터 웨어하우스 암호	필수 변경 사항
Cognos_admin	
드Wh	
dWh_INTERNAL(서버 커넥터 구성 UI를 사용하여 변경)	Insight 서버
Dwhuser(사용자)	
호스트	
인벤토리(서버 커넥터 구성 UI를 사용하여 변경됨)	Insight 서버
루트	

- DWH 서버 연결 구성 UI * 에서 암호 변경

다음 표에는 Lau의 사용자 암호와 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

Lau 암호	필수 변경 사항
획득	Insight 서버, RAU

서버 연결 구성 **UI**를 사용하여 **"inventory"** 및 **"dWh_internal"** 암호 변경

데이터 웨어하우스 UI를 사용하는 Insight 서버의 암호와 일치하도록 ""인벤토리" 또는 ""DIH_INTERNAL"" 암호를 변경해야 하는 경우

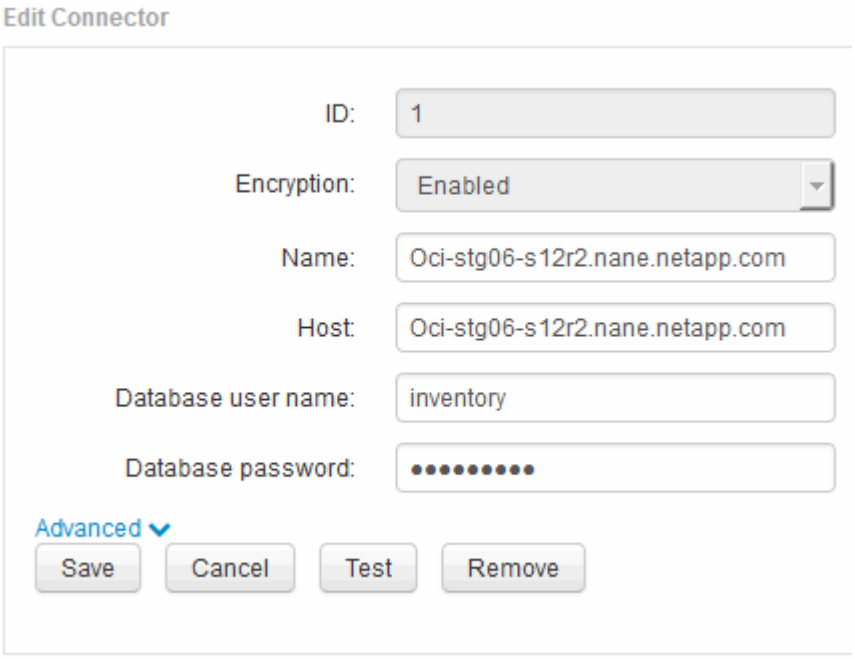
시작하기 전에

이 작업을 수행하려면 관리자로 로그인해야 합니다.

단계

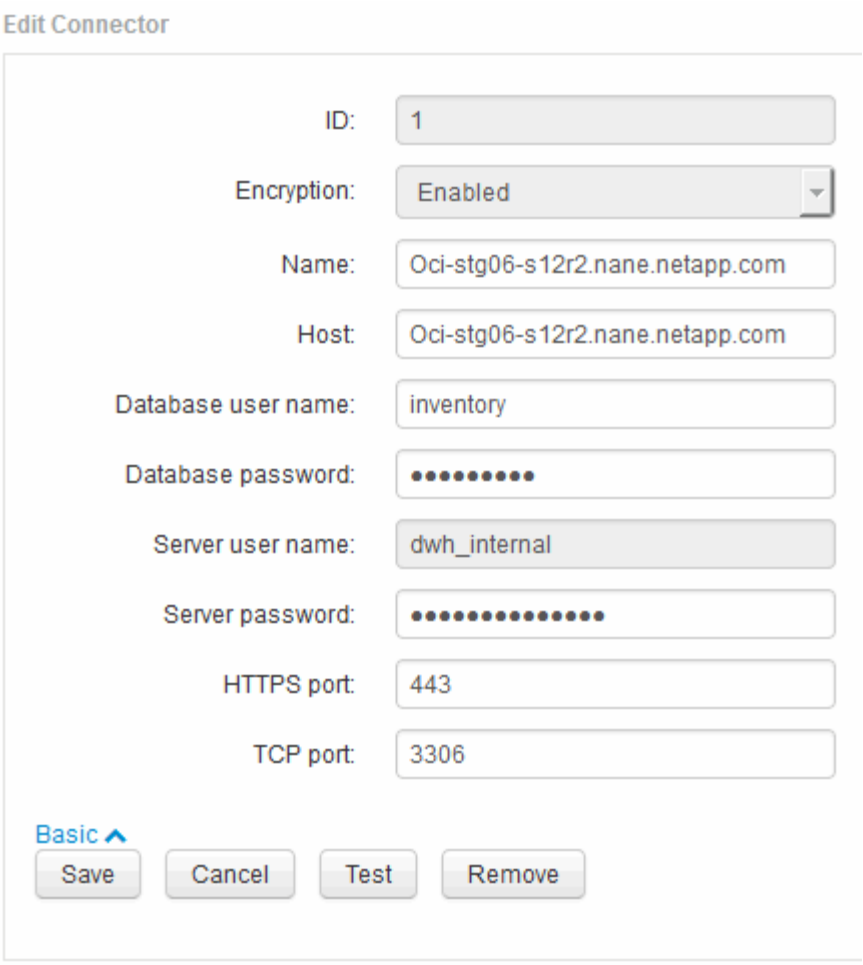
1. 에서 데이터 웨어하우스 포털에 로그인합니다 https://hostname/dwh여기서 hostname 은 OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 커넥터 * 를 클릭합니다.

   커넥터 편집 * 화면이 표시됩니다.



3. Database password * 필드에 새 ""Inventory"" 암호를 입력합니다.
4. 저장 * 을 클릭합니다
5. "dWh_INTERNAL" 암호를 변경하려면 * 고급 * 을 클릭합니다

   커넥터 고급 편집 화면이 표시됩니다.



6. 서버 암호 * 필드에 새 암호를 입력합니다.
7. 저장 을 클릭합니다.

ODBC 관리 도구를 사용하여 dWh 암호를 변경합니다

Insight 서버에서 dWh 사용자의 암호를 변경하면 데이터 웨어하우스 서버에서도 암호를 변경해야 합니다. ODBC 데이터 원본 관리자 도구를 사용하여 데이터 웨어하우스의 암호를 변경할 수 있습니다.

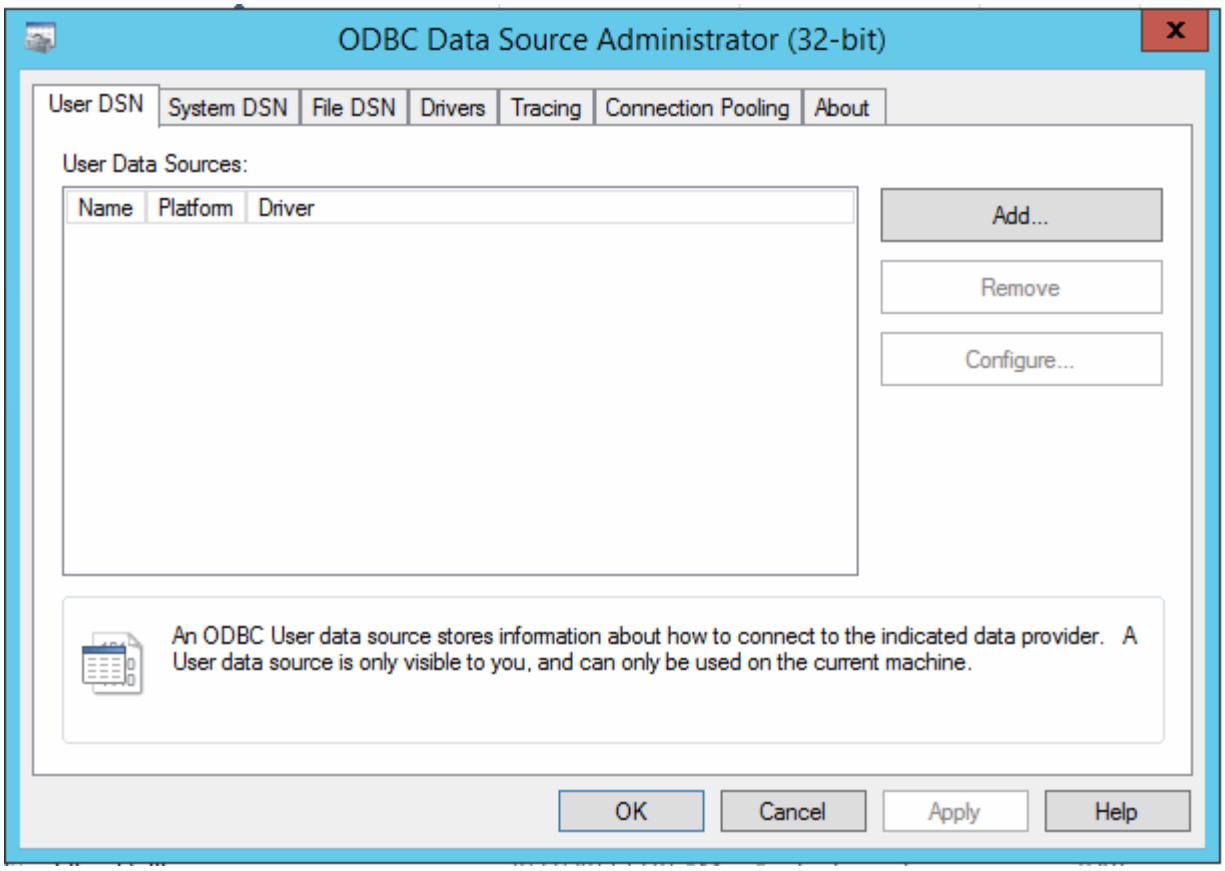
시작하기 전에

관리자 권한이 있는 계정을 사용하여 데이터 웨어하우스 서버에 원격으로 로그인해야 합니다.

단계

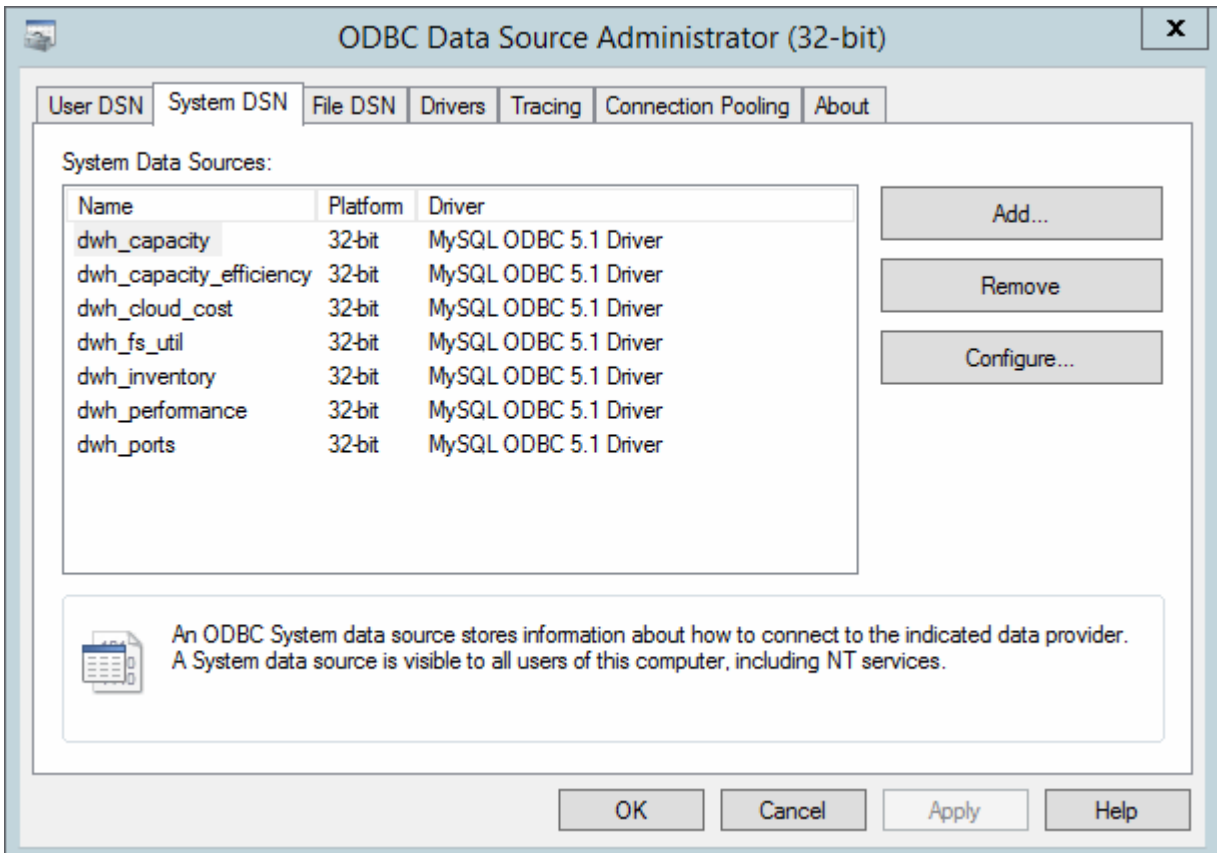
1. 해당 데이터 웨어하우스를 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 에서 ODBC 관리 도구에 액세스합니다 `C:\Windows\SysWOW64\odbcad32.exe`

   ODBC 데이터 원본 관리자 화면이 표시됩니다.



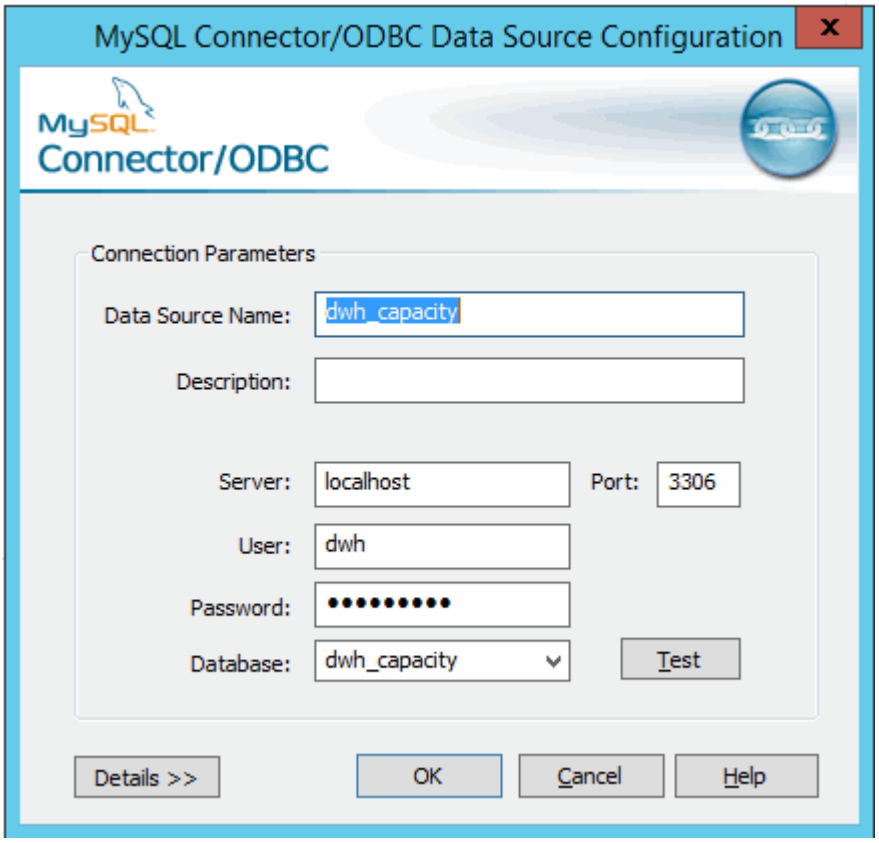
3. 시스템 DSN*을 클릭합니다

   시스템 데이터 소스가 표시됩니다.



4. 목록에서 OnCommand Insight 데이터 원본을 선택합니다.
5. 구성 * 을 클릭합니다

   데이터 소스 구성 화면이 표시됩니다.



6. 암호 * 필드에 새 암호를 입력합니다.