



Insight Security 를 참조하십시오 OnCommand Insight

NetApp
April 01, 2024

목차

Insight Security 를 참조하십시오	1
서버 키를 다시 입력합니다	1
획득 사용자 암호 변경	1
업그레이드 및 설치 고려 사항	1
복잡한 서비스 공급자 환경에서 키 관리	1
Insight 서버의 보안 관리	2
로컬 획득 장치의 보안 관리	4
RAU에 대한 보안 관리	6
데이터 웨어하우스의 보안 관리	7
OnCommand Insight 내부 사용자 암호 변경	9

Insight Security 를 참조하십시오

OnCommand Insight 7.3.1에서는 향상된 보안으로 Insight 환경을 운영할 수 있는 보안 기능이 도입되었습니다. 암호화, 암호 해싱의 개선, 암호를 암호화하고 해독하는 내부 사용자 암호 및 키 쌍 변경 기능이 포함되어 있습니다. Insight 환경의 모든 서버에서 이러한 기능을 관리할 수 있습니다.

Insight의 기본 설치에는 사용자 환경의 모든 사이트에서 동일한 키와 동일한 기본 암호를 공유하는 보안 구성이 포함됩니다. 중요 데이터를 보호하려면 설치 또는 업그레이드 후에 기본 키와 취득 사용자 암호를 변경하는 것이 좋습니다.

데이터 소스 암호화된 암호는 Insight Server 데이터베이스에 저장됩니다. 서버에 공개 키가 있으며 사용자가 WebUI 데이터 소스 구성 페이지에 암호를 입력할 때 암호를 암호화합니다. 서버에 Server 데이터베이스에 저장된 데이터 소스 암호를 해독하는 데 필요한 개인 키가 없습니다. 획득 장치(Lau, RAU)만 데이터 소스 암호를 해독하는 데 필요한 데이터 소스 개인 키를 가지고 있습니다.

서버 키를 다시 입력합니다

기본 키를 사용하면 환경에 보안 취약점이 발생합니다. 기본적으로 데이터 소스 암호는 Insight 데이터베이스에 암호화됩니다. 모든 Insight 설치에 공통적으로 사용되는 키를 사용하여 암호화됩니다. 기본 구성에서 NetApp에 전송된 Insight 데이터베이스에는 이론적으로 NetApp에 의해 암호 해독될 수 있는 암호가 포함되어 있습니다.

획득 사용자 암호 변경

기본 '획득' 사용자 암호를 사용하면 환경에 보안 취약점이 발생합니다. 모든 획득 장치는 ""획득" 사용자를 사용하여 서버와 통신합니다. 기본 암호가 있는 RA는 이론적으로 기본 암호를 사용하여 모든 Insight 서버에 연결할 수 있습니다.

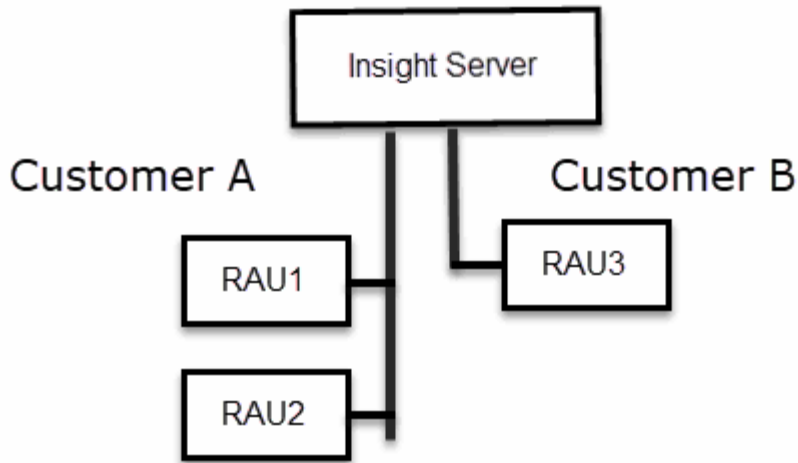
업그레이드 및 설치 고려 사항

Insight 시스템에 기본 보안 구성이 아닌 구성(암호 키를 다시 입력하거나 변경한 경우)이 포함된 경우 보안 구성을 백업해야 합니다. 새 소프트웨어를 설치하거나 소프트웨어를 업그레이드하는 경우 시스템을 기본 보안 구성으로 되돌립니다. 시스템이 기본 구성으로 복원되면 시스템이 올바르게 작동하려면 기본이 아닌 구성을 복원해야 합니다.

복잡한 서비스 공급자 환경에서 키 관리

서비스 공급자는 데이터를 수집하는 여러 OnCommand Insight 고객을 호스팅할 수 있습니다. 이 키는 Insight 서버의 여러 고객이 무단으로 고객 데이터에 액세스하지 못하도록 보호합니다. 각 고객의 데이터는 특정 키 쌍으로 보호됩니다.

이 Insight 구현은 다음 그림과 같이 구성할 수 있습니다.



이 구성에서는 각 고객에 대해 개별 키를 생성해야 합니다. 고객 A는 두 RA 모두에 대해 동일한 키를 필요로 합니다. 고객 B에는 단일 키 세트가 필요합니다.

고객 A의 암호화 키를 변경하는 단계:

1. RAU1을 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 보안 관리 도구를 시작합니다.
3. 기본 키를 대체하려면 암호화 키 변경 을 선택합니다.
4. 백업 을 선택하여 보안 구성의 백업 zip 파일을 생성합니다.
5. RAU2를 호스팅하는 서버에 원격 로그인을 수행합니다.
6. 보안 구성의 백업 zip 파일을 RAU2에 복사합니다.
7. 보안 관리 도구를 시작합니다.
8. 보안 백업을 RAU1에서 현재 서버로 복원합니다.

고객 B의 암호화 키를 변경하는 단계:

1. RAU3을 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 보안 관리 도구를 시작합니다.
3. 기본 키를 대체하려면 암호화 키 변경 을 선택합니다.
4. 백업 을 선택하여 보안 구성의 백업 zip 파일을 생성합니다.

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

단계

1. Insight 서버에 원격 로그인을 수행합니다.

2. 대화형 모드에서 보안 관리 도구를 시작합니다.

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

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

4. 서버 * 를 선택합니다.

다음 서버 구성 옵션을 사용할 수 있습니다.

◦ * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

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

◦ * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 서버 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다

◦ * 암호화 키 변경 *

프록시 사용자 암호, SMTP 사용자 암호, LDAP 사용자 암호 등을 암호화 또는 해독하는 데 사용되는 서버 암호화 키를 변경합니다.



암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 암호 업데이트 *

Insight에서 사용하는 내부 계정의 암호를 변경합니다. 다음 옵션이 표시됩니다.

- _내부
- 획득
- Cognos_admin
- DWh _ 내부
- 호스트
- 인벤토리
- 루트



암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

• * 기본값으로 재설정 *

키와 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

• * 종료 *

를 종료합니다 securityadmin 도구.

a. 변경할 옵션을 선택하고 화면의 지시를 따릅니다.

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

단계

1. Insight 서버에 원격 로그인을 수행합니다.
2. 대화형 모드에서 보안 관리 도구를 시작합니다.

◦ 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i

◦ Linux - /bin/oci-securityadmin.sh -i

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

4. Local Acquisition Unit(로컬 획득 장치) * 을 선택하여 Local Acquisition Unit(로컬 획득 장치) 보안 구성을 재구성합니다.

다음 옵션이 표시됩니다.

◦ * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

▪ 윈도우 - C:\Program Files\SANscreen\backup\vault

▪ Linux - /var/log/netapp/oci/backup/vault

◦ * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원을 사용하여 여러 서버의 패스워드와 키를 동기화할 수 있습니다. 예를 들어: - Lau에서 암호화 키 변경 - 볼트 백업 작성 - 각 RA에 볼트 백업을 복원합니다

◦ * 암호화 키 변경 *

장치 암호를 암호화 또는 해독하는 데 사용되는 AU 암호화 키를 변경합니다.



암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 암호 업데이트 *

'촬영' 사용자 계정의 암호를 변경합니다.



암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 기본값으로 재설정 *

획득 사용자 암호 및 획득 사용자 암호화 키를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

◦ * 종료 *

를 종료합니다 securityadmin 도구.

5. 구성할 옵션을 선택하고 화면의 지시를 따릅니다.

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 해당 사용자의 암호가 서버에서 변경된 경우 'acquisition' 사용자 암호를 업데이트하는 것입니다. 모든 RA와 Lau는 서버 '획득' 사용자의 암호와 동일한 암호를 사용하여 서버와 통신합니다.

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

RAU에서 보안 옵션을 관리하려면 다음 단계를 따르십시오.

단계

1. RAU를 실행 중인 서버에 원격 로그인을 수행한다
2. 대화형 모드에서 보안 관리 도구를 시작합니다.

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

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

RAU에 대한 메뉴가 표시됩니다.

- * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

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

- * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다

◦ * 암호화 키 변경 *

단말기 암호를 암호화 또는 해독하는 데 사용되는 RAU 암호화 키를 변경합니다.



암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 암호 업데이트 *

'촬영' 사용자 계정의 암호를 변경합니다.



암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 기본값으로 재설정 *

암호화 키 및 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

◦ * 종료 *

를 종료합니다 securityadmin 도구.

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

단계

1. 데이터 웨어하우스 서버에 원격 로그인을 수행합니다.
2. 대화형 모드에서 보안 관리 도구를 시작합니다.

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

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

데이터 웨어하우스에 대한 보안 관리 메뉴가 표시됩니다.

◦ * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 기본 위치에 파일을 배치합니다.

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

◦ * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다

를 누릅니다

◦ * 암호화 키 변경 *

커넥터 암호 및 SMPT 암호와 같은 암호를 암호화 또는 해독하는 데 사용되는 DWH 암호화 키를 변경합니다.

◦ * 암호 업데이트 *

특정 사용자 계정의 암호를 변경합니다.

- _내부
- 획득
- Cognos_admin
- 드Wh
- DWh _ 내부
- Dwhuser(사용자)
- 호스트
- 인벤토리
- 루트



dwhuser, hosts, inventory 또는 root 암호를 변경하면 SHA-256 암호 해싱을 사용할 수 있습니다. 이 옵션을 사용하려면 계정에 액세스하는 모든 클라이언트가 SSL 연결을 사용해야 합니다.

+

◦ * 기본값으로 재설정 *

암호화 키 및 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

◦ * 종료 *

를 종료합니다 securityadmin 도구.

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 UI를 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/dwh> 여기서 hostname 은 OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 커넥터 * 를 클릭합니다.

커넥터 편집 * 화면이 표시됩니다.

Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="••••••••"/>
Advanced ▼	
<input type="button" value="Save"/>	<input type="button" value="Cancel"/> <input type="button" value="Test"/> <input type="button" value="Remove"/>

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.

Edit Connector

ID:	1
Encryption:	Enabled
Name:	Oci-stg06-s12r2.nane.netapp.com
Host:	Oci-stg06-s12r2.nane.netapp.com
Database user name:	inventory
Database password:
Server user name:	dwh_internal
Server password:
HTTPS port:	443
TCP port:	3306

Basic ^

Save Cancel Test Remove

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.

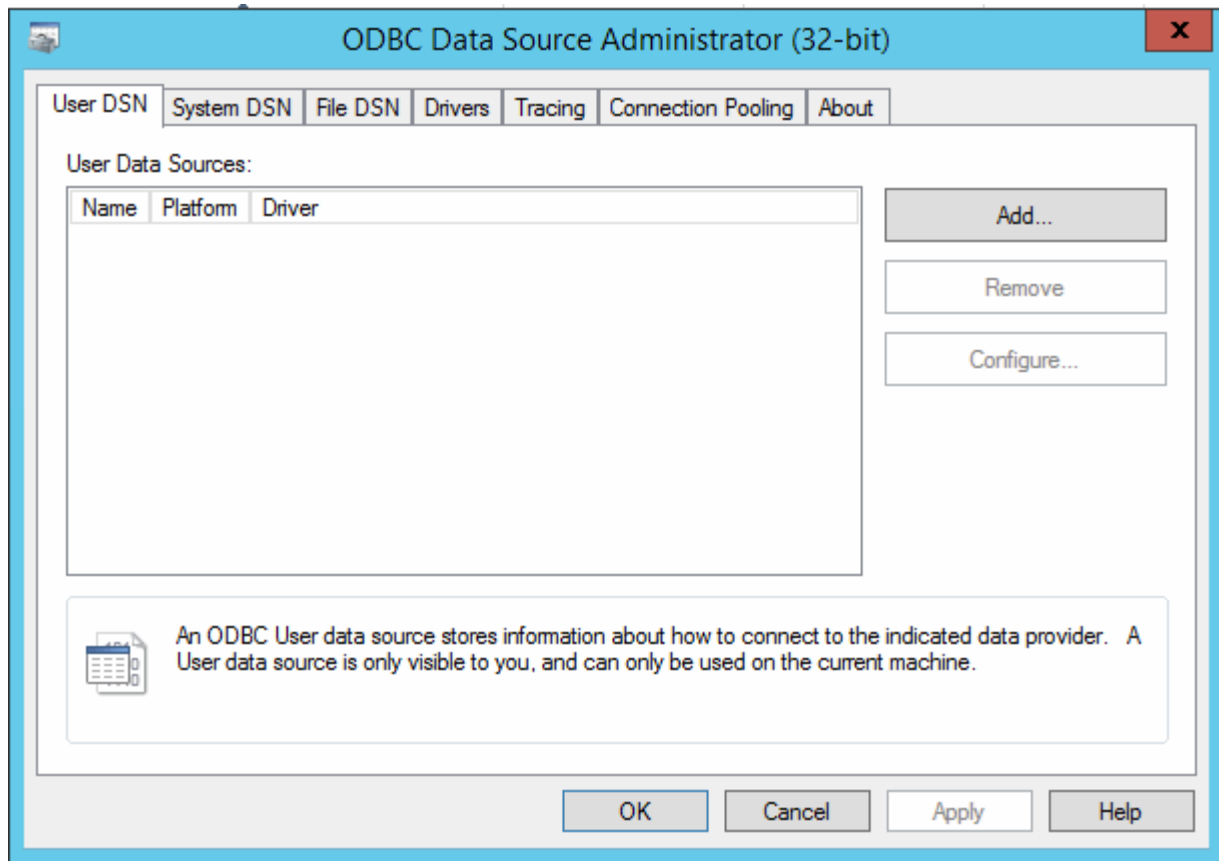
시작하기 전에

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

단계

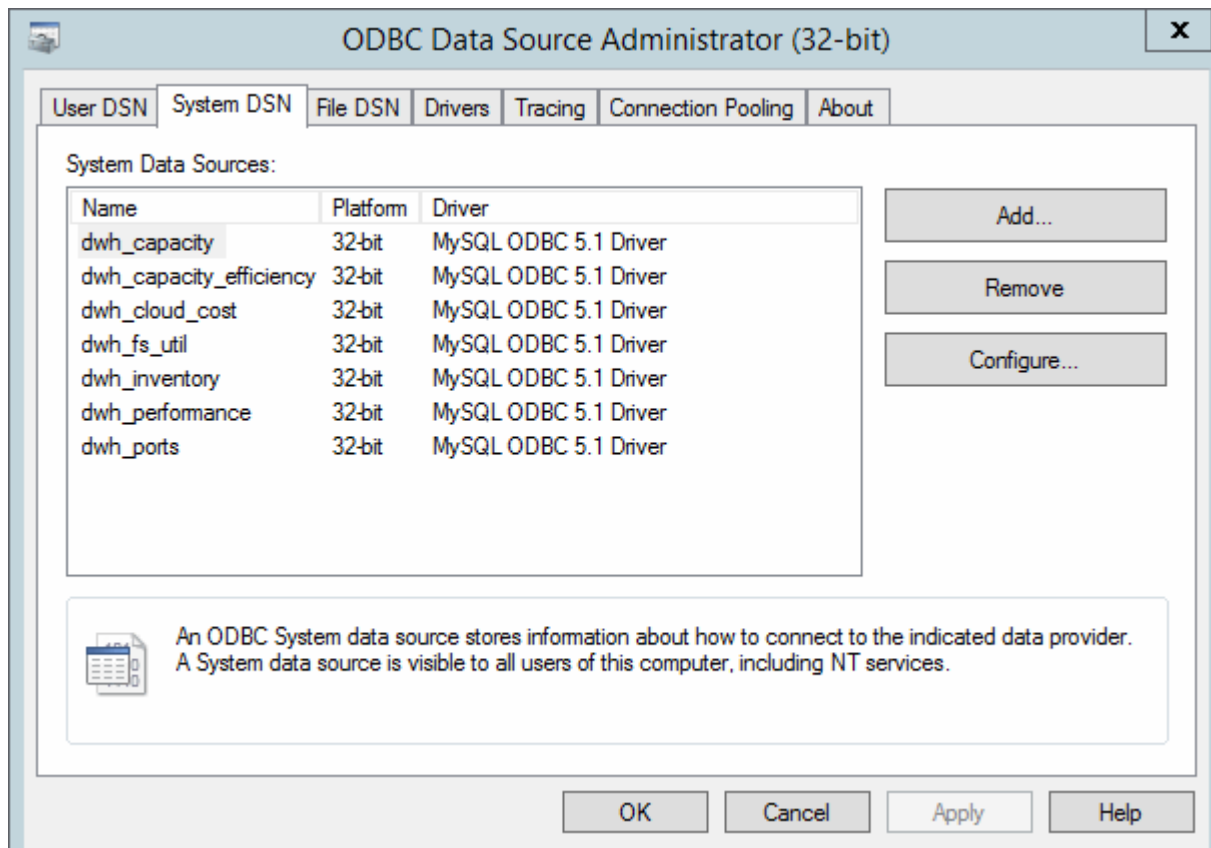
1. 해당 데이터 웨어하우스를 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 에서 ODBC 관리 도구에 액세스합니다 C:\Windows\SysWOW64\odbcad32.exe

ODBC 데이터 원본 관리자 화면이 표시됩니다.



3. 시스템 DSN*을 클릭합니다

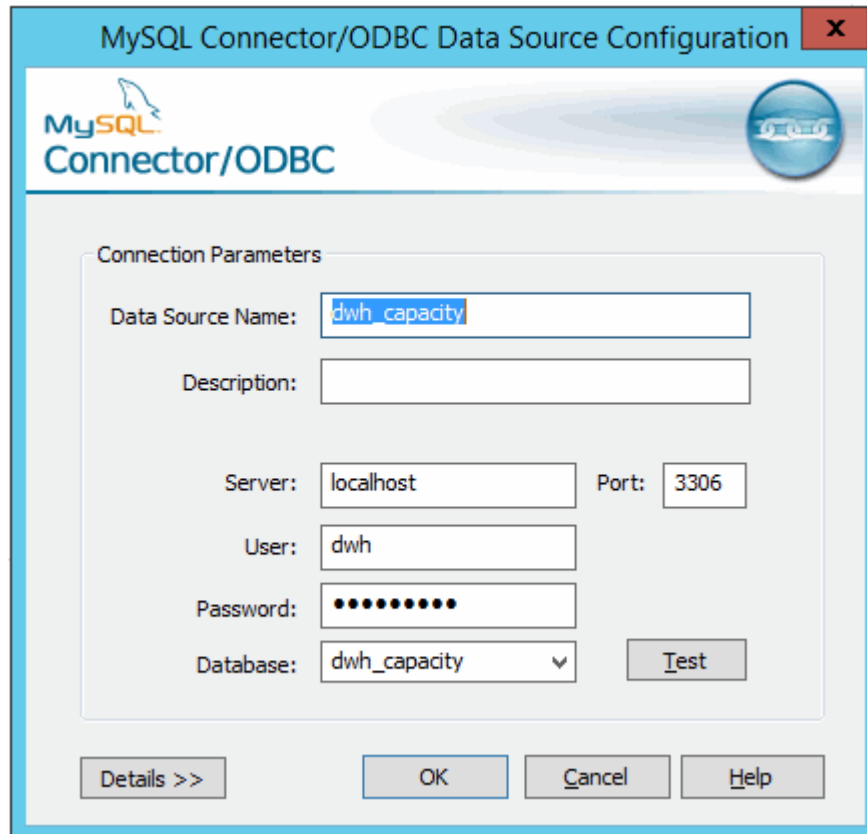
시스템 데이터 소스가 표시됩니다.



4. 목록에서 OnCommand Insight 데이터 원본을 선택합니다.

5. 구성 * 을 클릭합니다

데이터 소스 구성 화면이 표시됩니다.



The image shows the 'MySQL Connector/ODBC Data Source Configuration' dialog box. The title bar is blue with the text 'MySQL Connector/ODBC Data Source Configuration' and a red close button. The main area has a light blue header with the MySQL logo and 'Connector/ODBC'. Below this is a 'Connection Parameters' section with a light gray background. It contains the following fields: 'Data Source Name' (text box with 'dwh_capacity'), 'Description' (empty text box), 'Server' (text box with 'localhost'), 'Port' (text box with '3306'), 'User' (text box with 'dwh'), 'Password' (password box with 10 dots), and 'Database' (dropdown menu with 'dwh_capacity' selected). There is a 'Test' button next to the Database dropdown. At the bottom of the dialog are four buttons: 'Details >>', 'OK', 'Cancel', and 'Help'.

6. 암호 * 필드에 새 암호를 입력합니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.