



Insight Security (SecurityAdmin Tool)

OnCommand Insight

NetApp

October 24, 2024

Índice

Ferramenta SecurityAdmin	1
O que é a ferramenta SecurityAdmin?	1
Modos de execução	1
Comandos	2
Ações coordenadas	4
Executando a ferramenta Security Admin - linha de comando	6
Executar a ferramenta de administração de segurança - modo interativo	10
Gerenciamento da segurança no servidor Insight	20
Gestão da segurança na unidade de aquisição local	20
Gerenciamento de segurança em uma RAU	21
Gestão da segurança no Data Warehouse	21
Alterando senhas internas de usuário do OnCommand Insight	21

Ferramenta SecurityAdmin

O OnCommand Insight fornece recursos que permitem que os ambientes Insight operem com segurança aprimorada. Esses recursos incluem criptografia, hash de senha e a capacidade de alterar senhas internas de usuário e pares de chaves que criptografam e descriptografam senhas. Você pode gerenciar esses recursos em todos os servidores no ambiente Insight usando a **SecurityAdmin Tool**.

O que é a ferramenta SecurityAdmin?

A ferramenta de administração de segurança suporta alterações no conteúdo dos cofres, bem como fazer alterações coordenadas na instalação do OnCommand Insight.

Os principais usos para a ferramenta SecurityAdmin são para **Backup e Restore** da configuração de segurança (ou seja, Vault) e senhas. Por exemplo, você pode fazer backup do Vault em uma Unidade de aquisição local e restaurá-lo em uma Unidade de aquisição remota, garantindo a coordenação de senhas em todo o seu ambiente. Ou se você tiver vários servidores OnCommand Insight em seu ambiente, talvez queira fazer um backup do Vault do servidor e restaurá-lo para outros servidores para manter as senhas iguais. Estes são apenas dois exemplos de como o SecurityAdmin pode ser usado para garantir a coesão em seus ambientes.



É altamente recomendável **fazer backup do Vault** sempre que você fizer backup de um banco de dados OnCommand Insight. Se não o fizer, pode resultar em perda de acesso.

A ferramenta fornece os modos **interactive** e **command line**.

Muitas operações da SecurityAdmin Tool alteram o conteúdo do Vault e também fazem alterações na instalação, garantindo que o Vault e a instalação permaneçam sincronizados.

Por exemplo,

- Quando você altera uma senha de usuário do Insight, a entrada do usuário na tabela SANscreen.Users será atualizada com o novo hash.
- Quando você altera a senha de um usuário MySQL, a instrução SQL apropriada será executada para atualizar a senha do usuário na instância MySQL.

Em algumas situações, haverá várias alterações feitas na instalação:

- Quando você modifica o usuário dwh MySQL, além de atualizar a senha no banco de dados MySQL, várias entradas de Registro para ODBC também serão atualizadas.

Nas seções a seguir, o termo "mudanças coordenadas" é usado para descrever essas mudanças.

Modos de execução

- Operação normal/padrão - o Serviço de servidor SANscreen deve estar em execução

Para o modo de execução padrão, a ferramenta SecurityAdmin requer que o serviço **servidor SANscreen** esteja em execução. O servidor é usado para autenticação, e muitas alterações coordenadas na instalação são feitas fazendo chamadas para o servidor.

- Operação direta - o Serviço de servidor SANscreen pode estar em execução ou parado.

Quando executado em uma instalação do OCI Server ou DWH, a ferramenta também pode ser executada no modo "direto". Neste modo, a autenticação e as alterações coordenadas são realizadas usando o banco de dados. O serviço servidor não é usado.

O funcionamento é o mesmo que o modo normal, com as seguintes exceções:

- A autenticação é suportada apenas para utilizadores de administração que não sejam de domínio. (Usuários cuja senha e funções estão no banco de dados, não LDAP).
- A operação "Substituir chaves" não é suportada.
- A etapa de re-criptografia da restauração do Vault é ignorada.
- A ferramenta também pode ser executada mesmo quando o acesso ao servidor e ao banco de dados não é possível (por exemplo, porque a senha raiz no cofre está incorreta).

Quando executado neste modo, a autenticação não é possível e, portanto, nenhuma operação com uma alteração coordenada para a instalação pode ser executada.

O modo de recuperação pode ser utilizado para:

- determine quais entradas do vault estão erradas (usando a operação verificar)
- substitua a senha raiz incorreta pelo valor correto. (Isso não altera a senha. O utilizador tem de introduzir a palavra-passe atual.)



Se a senha raiz no cofre estiver incorreta e a senha não for conhecida e não houver backup do cofre com a senha raiz correta, a instalação não poderá ser recuperada usando a ferramenta SecurityAdmin. A única maneira de recuperar a instalação é redefinir a senha da instância MySQL seguindo o procedimento documentado em <https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html>. Depois de executar o procedimento de reinicialização, use a operação de senha armazenada correta para inserir a nova senha no cofre.

Comandos

Comandos irrestritos

Comandos irrestritos fazem quaisquer alterações coordenadas na instalação (exceto armazenamentos confiáveis). Comandos irrestritos podem ser executados sem autenticação do usuário.

Comando	Descrição
backup-vault	<p>Crie um arquivo zip contendo o cofre. O caminho relativo para os arquivos do Vault corresponderá ao caminho do Vault relativo à raiz da instalação.</p> <ul style="list-style-type: none"> • wildfly/standalone/configuration/vault/* • acq/conf/vault/* <p>Observe que é altamente recomendável fazer backup do Vault sempre que você fizer backup de um banco de dados do OnCommand Insight.</p>

verifique se há teclas padrão	Verifique se as chaves do Vault correspondem às do Vault padrão usado em instâncias anteriores a 7.3.16.
palavra-passe guardada correta	Substitua uma senha (incorreta) armazenada no cofre pela senha correta conhecida pelo usuário. Isso pode ser usado quando o Vault e a instalação não são consistentes. Observe que não altera a senha real na instalação.
	Altere a senha usada para um armazenamento de confiança e armazene a nova senha no cofre. A palavra-passe atual da loja de confiança tem de ser "conhecida".
verifique-keystore	verifique se os valores no cofre estão corretos: <ul style="list-style-type: none"> • Para usuários do OCI, o hash da senha corresponde ao valor no banco de dados • Para usuários MySQL, pode ser feita uma conexão de banco de dados • para keystores, o keystore pode ser carregado e suas chaves (se houver) lidas
teclas de lista	listar as entradas no cofre (sem mostrar o valor armazenado)

Comandos restritos

A autenticação é necessária para qualquer comando não oculto que faça alterações coordenadas na instalação:

Comando	Descrição
restaurar-vault-backup	<p>Substitui o Vault atual pelo Vault contido no arquivo de backup especificado.</p> <p>Executa todas as ações coordenadas para atualizar a instalação para corresponder às senhas no cofre restaurado:</p> <ul style="list-style-type: none"> • Atualize as senhas de usuário de comunicação OCI • Atualize as senhas do usuário MySQL, incluindo root • para cada keystore, se a senha do keystore for "conhecida", atualize o keystore usando as senhas do cofre restaurado. <p>Quando executado no modo normal, também lê cada valor criptografado da instância, descriptografa-o usando o serviço de criptografia do Vault atual, recriptografa-o usando o serviço de criptografia do Vault restaurado e armazena o valor recriptografado.</p>

sincronize-com-cofre	<p>Executa todas as ações coordenadas para atualizar a instalação para corresponder às senhas de usuário no cofre restaurado:</p> <ul style="list-style-type: none"> • Atualiza as senhas de usuário de comunicação OCI • Atualiza as senhas do usuário MySQL, incluindo root
alterar palavra-passe	Altera a senha no cofre e executa as ações coordenadas.
substitua as chaves	Crie um novo cofre vazio (que terá chaves diferentes do existente). Em seguida, copie as entradas do Vault atual para o novo Vault. Em seguida, lê cada valor encriptado da instância, descripta-o utilizando o serviço de encriptação do cofre atual, encripta-o novamente utilizando o serviço de encriptação do cofre restaurado e armazena o valor recriptado.

Ações coordenadas

Cofre do servidor

_interno	atualizar hash de senha para usuário no banco de dados
aquisição	<p>atualizar hash de senha para usuário no banco de dados</p> <p>se o cofre de aquisição estiver presente, atualize também a entrada no cofre de aquisição</p>
dwh_internal	atualizar hash de senha para usuário no banco de dados
cognos_admin	<p>atualizar hash de senha para usuário no banco de dados</p> <p>Se DWH e Windows, atualize SANSscreen/cognos/analytics/Configuration/SANSscreenAP.properties para definir a propriedade cognos.admin como a senha.</p>
raiz	Execute SQL para atualizar a senha do usuário na instância do MySQL
inventário	Execute SQL para atualizar a senha do usuário na instância do MySQL

dwh	<p>Execute SQL para atualizar a senha do usuário na instância do MySQL</p> <p>Se DWH e Windows, atualize o Registro do Windows para definir as seguintes entradas relacionadas a ODBC para a nova senha:</p> <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_Capacity/PWD • HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC/dwh_Capacity_Efficiency/PWD • HKEY_LOCAL_MACHINE_SOFTWARE/Wow6432Node ODBC.INI/dwh_fs_util/PWD • HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_inventory/PWD • HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_performance/PWD • HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC/dwh_ports/PWD • HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_sa/PWD • HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node ODBC.INI/dwh_cloud_cost/PWD
dwhuser	Execute SQL para atualizar a senha do usuário na instância do MySQL
hosts	Execute SQL para atualizar a senha do usuário na instância do MySQL
keystore_password	reescreva o keystore com a nova senha - wildfly/standalone/configuration/server.keystore
truststore_password	reescreva o keystore com a nova senha - wildfly/standalone/configuration/server.truststore
key_password	reescreva o keystore com a nova senha - wildfly/standalone/configuration/sso.jks
cognos_archive	nenhum

Aquisição do Vault

aquisição	nenhum
truststore_password	reescreva o keystore com a nova senha (se existir) - acq/conf/cert/client.keystore

Executando a ferramenta Security Admin - linha de comando

A sintaxe para executar a ferramenta SA no modo de linha de comando é:

```
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
```

Notas:

- A opção "-i" pode não estar presente na linha de comando (uma vez que seleciona o modo interativo).
- para as opções "-s" e "-au":
 - "-s" não é permitido numa RAU
 - "-au" não é permitido na DWH
 - se nenhum dos dois estiver presente, então
 - O cofre do servidor é selecionado em servidor, DWH e Dual
 - O cofre de aquisição é selecionado na RAU
- As opções -lu e -lp são usadas para autenticação do usuário.
 - Se o <user> for especificado e o <password> não for, o usuário será solicitado a digitar a senha.
 - Se o <user> não for fornecido e a autenticação for necessária, o usuário será solicitado a fornecer o <user> e o <password>.

Comandos:

Comando	Utilização
palavra-passe guardada correta	<pre>securityadmin [-s</pre>

<p>-au] [-db] -pt <key> [<value>]</p> <p>where</p> <p>-pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value</p>	<p>backup-vault</p>
<p>securityadmin [-s</p>	<p>-au] [-db] -b [<backup-dir>]</p> <p>where</p> <p>-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</p>
<p>backup-vault</p>	<p>securityadmin [-s</p>
<p>-au] [-db] -ub <backup-file></p> <p>where</p> <p>-ub specified command ("upgrade-backup") <backup-file> The location to write the backup file</p>	<p>teclas de lista</p>
<p>securityadmin [-s</p>	<p>-au] [-db] -l</p> <p>where</p> <p>-l specified command</p>

<p>teclas de verificação</p>	<pre>securityadmin [-s</pre>
<p>-au] [-db] -ck</p> <p>where</p> <p>-ck specified command</p> <p>exit code: 1 error 2 default key(s) 3 unique keys</p> <pre>securityadmin [-s</pre>	<p>verificar-keystore (servidor)</p>
<pre>securityadmin [-s] [-db] -v</pre> <p>where</p> <p>-v specified command</p>	<p>atualização</p>
<pre>securityadmin [-s</pre>	<p>-au] [-db] [-lu <user>] [-lp <password>] -u</p> <p>where</p> <p>-u specified command</p> <p>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</p> <pre>securityadmin [-s</pre>
<p>substitua as chaves</p>	<pre>securityadmin [-s</pre>

<p>-au] [-db] [-lu <user>] [-lp <password>] -rk</p> <p>where</p> <p>-rk specified command</p> <div data-bbox="136 333 461 403" style="border: 1px solid #ccc; height: 33px; width: 100%;"></div>	<p>restaurar-vault-backup</p>
<div data-bbox="136 447 461 588" style="border: 1px solid #ccc; padding: 5px;"> <p>securityadmin [-s</p> </div>	<p>-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file></p> <p>where</p> <p>-r specified command <backup-file> the backup file location</p> <div data-bbox="480 646 1484 716" style="border: 1px solid #ccc; height: 33px; width: 100%;"></div>
<p>alterar palavra-passe (servidor)</p>	<div data-bbox="480 758 1484 1220" style="border: 1px solid #ccc; padding: 10px;"> <p>securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]</p> <p>where</p> <p>-up specified command ("update-password")</p> <p>-un <user> entry ("user") name to update</p> <p>-p <password> new password. If <password not supplied, user will be prompted.</p> <p>-sh for mySQL user, use strong hash</p> </div>
<p>alterar palavra-passe para utilizador de aquisição (aquisição)</p>	<div data-bbox="480 1268 1484 1646" style="border: 1px solid #ccc; padding: 10px;"> <p>securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]</p> <p>where</p> <p>-up specified command ("update-password")</p> <p>-p <password> new password. If <password not supplied, user will be prompted.</p> </div>

<p>alterar-senha para truststore_password (aquisição)</p>	<pre>securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]</pre> <p>where</p> <pre>-utp specified command ("update-truststore-password")</pre> <pre>-p <password> new password. If <password not supplied, user will be prompted.</pre>
<p>sincronizar com cofre (servidor)</p>	<pre>securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file></pre> <p>where</p> <pre>-sv specified command</pre>

Executar a ferramenta de administração de segurança - modo interativo

Interativo - Menu principal

Para executar a ferramenta SA no modo interativo, digite o seguinte comando:

```
securityadmin -i
```

Em um servidor ou instalação dupla, o SecurityAdmin solicitará ao usuário que selecione o servidor ou a unidade de aquisição local.

Detectados nós de servidor e Unidade de aquisição! Selecione o nó cuja segurança precisa ser reconfigurada:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

No DWH, "Server" (servidor) é selecionado automaticamente. Numa AU remota, a opção "Acquisition Unit" (Unidade de aquisição) será selecionada automaticamente.

Interactive - servidor: Recuperação de senha root

No modo servidor, a ferramenta SecurityAdmin primeiro verificará se a senha raiz armazenada está correta. Caso contrário, a ferramenta exibirá a tela de recuperação de senha raiz.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Se a opção 1 estiver selecionada, o usuário será solicitado a digitar a senha correta.

```
Enter password (blank = don't change)
Enter correct password for 'root':
Se for introduzida a palavra-passe correta, é apresentado o seguinte.
```

```
Password verified. Vault updated
Pressionar ENTER exibirá o menu irrestrito do servidor.
```

Se for introduzida a palavra-passe errada, será apresentado o seguinte

```
Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Premir ENTER regressa ao menu de recuperação.
```

Se a opção 2 estiver selecionada, o usuário será solicitado a fornecer o nome de um arquivo de backup a partir do qual ler a senha correta:

```
Enter Backup File Location:
Se a senha do backup estiver correta, será exibido o seguinte.
```

```
Password verified. Vault updated
Pressionar ENTER exibirá o menu irrestrito do servidor.
```

Se a palavra-passe na cópia de segurança estiver incorreta, será apresentado o seguinte

```
Password verification failed - Access denied for user 'root'@'localhost'  
(using password: YES)  
Premir ENTER regressa ao menu de recuperação.
```

Interactive - servidor: Senha correta

A ação "corrigir senha" é usada para alterar a senha armazenada no cofre para que ela corresponda à senha real exigida pela instalação. Este comando é útil em situações em que uma mudança na instalação foi feita por algo diferente da ferramenta securityadmin. Os exemplos incluem:

- A senha de um usuário SQL foi modificada pelo acesso direto ao MySQL.
- Um keystore é substituído ou a senha de um keystore é alterada usando keytool.
- Um banco de dados OCI foi restaurado e esse banco de dados tem senhas diferentes para os usuários internos

"Corrigir senha" primeiro solicitará ao usuário que selecione a senha que deseja armazenar o valor correto.

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:

Depois de selecionar qual entrada corrigir, o usuário é solicitado a fornecer o valor.

- 1 - Enter {user} password
- 2 - Get {user} password from vault backup
- 9 - Exit

Enter your choice:

Se a opção 1 estiver selecionada, o usuário será solicitado a digitar a senha correta.

```
Enter password (blank = don't change)
Enter correct password for '{user}':
Se for introduzida a palavra-passe correta, é apresentado o seguinte.
```

```
Password verified. Vault updated
Pressionar ENTER retornará ao menu irrestrito do servidor.
```

Se for introduzida a palavra-passe errada, será apresentado o seguinte

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

Pressionar ENTER retornará ao menu irrestrito do servidor.

Se a opção 2 estiver selecionada, o usuário será solicitado a fornecer o nome de um arquivo de backup a partir do qual ler a senha correta:

```
Enter Backup File Location:
Se a senha do backup estiver correta, será exibido o seguinte.
```

```
Password verified. Vault updated
Pressionar ENTER exibirá o menu irrestrito do servidor.
```

Se a palavra-passe na cópia de segurança estiver incorreta, será apresentado o seguinte

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

Pressionar ENTER exibirá o menu irrestrito do servidor.

Interativo - servidor: Verifique o conteúdo do Vault

Verificar o conteúdo do Vault verificará se o Vault tem chaves que correspondem ao Vault padrão distribuído com versões anteriores do OCI e verificará se cada valor no Vault corresponde à instalação.

Os resultados possíveis para cada chave são:

OK	O valor do cofre está correto
Não verificado	O valor não pode ser verificado em relação à instalação

RUIM	O valor não corresponde à instalação
Em falta	Falta uma entrada esperada.

```
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
```

Interactive - servidor: Backup

O backup solicitará o diretório no qual o arquivo zip de backup deve ser armazenado. O diretório já deve existir e o nome do arquivo será ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip.

```
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
```

Interactive - servidor: Login

A ação de login é usada para autenticar um usuário e obter acesso a operações que modificam a instalação. O usuário deve ter Privileges de administrador. Ao executar com o servidor, qualquer usuário admin pode ser usado; ao executar no modo direto, o usuário deve ser um usuário local em vez de um usuário LDAP.

```
Authenticating via server. Enter user and password
```

```
UserName: admin
```

```
Password:
```

ou

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

```
UserName: admin
```

```
Password:
```

Se a senha estiver correta e o usuário for um usuário admin, o menu restrito será exibido.

Se a palavra-passe estiver incorreta, será apresentado o seguinte:

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

```
UserName: admin
```

```
Password:
```

```
Login Failed!
```

Se o usuário não for um administrador, o seguinte será exibido:

```
Authenticating via server. Enter user and password
```

```
UserName: user
```

```
Password:
```

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

Interativo - servidor: Menu restrito

Depois de o utilizador iniciar sessão, a ferramenta apresenta o Menu restrito.

```
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 - servidor: Alterar senha

A ação "Change Password" (alterar palavra-passe) é utilizada para alterar uma palavra-passe de instalação para um novo valor.

"Change Password" (alterar palavra-passe) solicitará primeiro ao utilizador que selecione a palavra-passe que pretende alterar.

```
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:
```

Depois de selecionar qual entrada corrigir, se o usuário for um usuário MySQL, o usuário será perguntado se deseja hash forte para a senha

```
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
```

Em seguida, o usuário é solicitado a fornecer a nova senha.

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

Se for introduzida uma palavra-passe não vazia, é pedido ao utilizador que confirme a palavra-passe.

```
New Password for '{user}':  
  
Confirm New Password for '{user}':  
  
Password successfully updated for 'dwhuser'!
```

Se a alteração não for bem-sucedida, o erro ou a exceção serão exibidos.

Interactive - servidor: Restauração

Interactive - servidor: Alterar chaves de criptografia

A ação alterar chaves de criptografia substituirá a chave de criptografia usada para criptografar as entradas do Vault e substituirá a chave de criptografia usada para o serviço de criptografia do Vault. Como a chave do serviço de criptografia é alterada, os valores criptografados no banco de dados serão recriptografados; eles serão lidos, descriptografados com a chave atual, criptografados com a nova chave e salvos de volta ao banco de dados.

Esta ação não é suportada no modo direto, uma vez que o servidor fornece a operação de recriptação para algum conteúdo de base de dados.

```
Replace encryption key with new key and update encrypted database values  
  
Confirm (y/N): y  
  
Change Encryption Keys succeeded! Restart 'Server' Service!
```

Interactive - servidor: Corrigir instalação

A ação Fix Installation atualizará a instalação. Todas as senhas de instalação que podem ser alteradas através da ferramenta securityadmin, exceto root, serão definidas para as senhas no cofre.

- As senhas dos usuários internos do OCI serão atualizadas.
- As senhas dos usuários MySQL, exceto root, serão atualizadas.
- As senhas dos keystores serão atualizadas.

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

Confirm: (y/N): y

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

A ação irá parar na primeira atualização mal sucedida e apresentar o erro ou exceção.

Gerenciamento da segurança no servidor Insight

A `securityadmin` ferramenta permite gerenciar opções de segurança no servidor Insight. O gerenciamento de segurança inclui alterar senhas, gerar novas chaves, salvar e restaurar configurações de segurança criadas por você ou restaurar configurações para as configurações padrão.

Sobre esta tarefa

Você usa a `securityadmin` ferramenta para gerenciar a segurança:

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

Consulte "[SecurityAdmin](#)"a documentação para obter mais informações.

Gestão da segurança na unidade de aquisição local

A `securityadmin` ferramenta permite gerenciar opções de segurança no usuário de aquisição local (LAU). O gerenciamento de segurança inclui o gerenciamento de chaves e senhas, salvar e restaurar configurações de segurança que você cria ou restaura as configurações padrão.

Antes de começar

Você deve ter `admin` o Privileges para executar tarefas de configuração de segurança.

Sobre esta tarefa

Você usa a `securityadmin` ferramenta para gerenciar a segurança:

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

Consulte "[Ferramenta SecurityAdmin](#)"as instruções para obter mais informações.

Gerenciamento de segurança em uma RAU

A `securityadmin` ferramenta permite gerenciar opções de segurança em RAUs. Talvez seja necessário fazer backup ou restaurar uma configuração de cofre, alterar chaves de criptografia ou atualizar senhas para as unidades de aquisição.

Sobre esta tarefa

Você usa a `securityadmin` ferramenta para gerenciar a segurança:

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

Um cenário para atualizar a configuração de segurança para o LAU/RAU é atualizar a senha do usuário 'aquisição' quando a senha para esse usuário tiver sido alterada no servidor. A LAU e todas as RAUs usam a mesma senha que a do usuário de 'aquisição' do servidor para se comunicar com o servidor.

O utilizador de 'aquisição' só existe no servidor Insight. A RAU ou LAU faz login como esse usuário quando eles se conectam ao servidor.

Consulte "[Ferramenta SecurityAdmin](#)" as instruções para obter mais informações.

Gestão da segurança no Data Warehouse

A `securityadmin` ferramenta permite gerenciar opções de segurança no servidor Data Warehouse. O gerenciamento de segurança inclui a atualização de senhas internas para usuários internos no servidor DWH, a criação de backups da configuração de segurança ou a restauração de configurações para as configurações padrão.

Sobre esta tarefa

Você usa a `securityadmin` ferramenta para gerenciar a segurança:

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

Consulte "[SecurityAdmin](#)" a documentação para obter mais informações.

Alterando senhas internas de usuário do OnCommand Insight

As políticas de segurança podem exigir que você altere as senhas em seu ambiente OnCommand Insight. Algumas das senhas em um servidor existem em um servidor diferente no ambiente, exigindo que você altere a senha em ambos os servidores. Por exemplo, quando você altera a senha do usuário "inventário" no Insight Server, você deve corresponder à senha do usuário "inventário" no conector do servidor do Data Warehouse configurado para esse Insight Server.

Antes de começar



Você deve entender as dependências das contas de usuário antes de alterar senhas. A falha na atualização de senhas em todos os servidores necessários resultará em falhas de comunicação entre os componentes do Insight.

Sobre esta tarefa

A tabela a seguir lista as senhas de usuário internas do Insight Server e lista os componentes do Insight que têm senhas dependentes que precisam corresponder à nova senha.

Senhas do Insight Server	Alterações necessárias
_interno	
aquisição	LAU, RAU
dwh_internal	Armazém de dados
hosts	
inventário	Armazém de dados
raiz	

A tabela a seguir lista as senhas de usuário internas do Data Warehouse e lista os componentes do Insight que têm senhas dependentes que precisam corresponder à nova senha.

Senhas do Data Warehouse	Alterações necessárias
cognos_admin	
dwh	
dwh_internal (alterado usando a IU de configuração do conector do servidor)	Servidor Insight
dwhuser	
hosts	
Inventário (alterado usando a IU de configuração do conector do servidor)	Servidor Insight
raiz	

Alterando senhas na IU de Configuração da conexão do servidor DWH

A tabela a seguir lista a senha do usuário para a LAU e lista os componentes do Insight que têm senhas dependentes que precisam corresponder à nova senha.

Palavras-passe LAU	Alterações necessárias
aquisição	Insight Server, RAU

Alterar as senhas "inventário" e "dwh_internal" usando a IU de Configuração de conexão do servidor

Se você precisar alterar as senhas "inventário" ou "dwh_internal" para corresponder às do servidor Insight, use a IU do Data Warehouse.

Antes de começar

Você deve estar conectado como administrador para executar esta tarefa.

Passos

1. Faça login no Portal do Armazém de dados em <https://hostname/dwh>, onde hostname é o nome do sistema onde o Armazém de dados OnCommand Insight está instalado.
2. No painel de navegação à esquerda, clique em **Connectors**.

É apresentado o ecrã **Edit Connector** (Editar conetor).

Edit Connector

The screenshot shows the 'Edit Connector' form with the following fields and values:

- ID: 1
- Encryption: Enabled
- Name: Oci-stg06-s12r2.nane.netapp.com
- Host: Oci-stg06-s12r2.nane.netapp.com
- Database user name: inventory
- Database password: [masked]

At the bottom of the form, there is an 'Advanced' dropdown menu and four buttons: Save, Cancel, Test, and Remove.

3. Insira uma nova senha de "inventário" para o campo **Senha do banco de dados**.
4. Clique em **Salvar**
5. Para alterar a senha "dWH_internal", clique em **Avançado**.

É apresentado o ecrã Edit Connector Advanced (Editar conetor avançado).

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="....."/>
Server user name:	<input type="text" value="dwh_internal"/>
Server password:	<input type="password" value="....."/>
HTTPS port:	<input type="text" value="443"/>
TCP port:	<input type="text" value="3306"/>

Basic ^

6. Digite a nova senha no campo **Senha do servidor**:

7. Clique em Save (Guardar).

Alterando a senha dwh usando a ferramenta Administração ODBC

Quando alterar a palavra-passe para o utilizador dwh no servidor Insight, a palavra-passe também tem de ser alterada no servidor Data Warehouse. Você usa a ferramenta Administrador de origem de dados ODBC para alterar a senha no Data Warehouse.

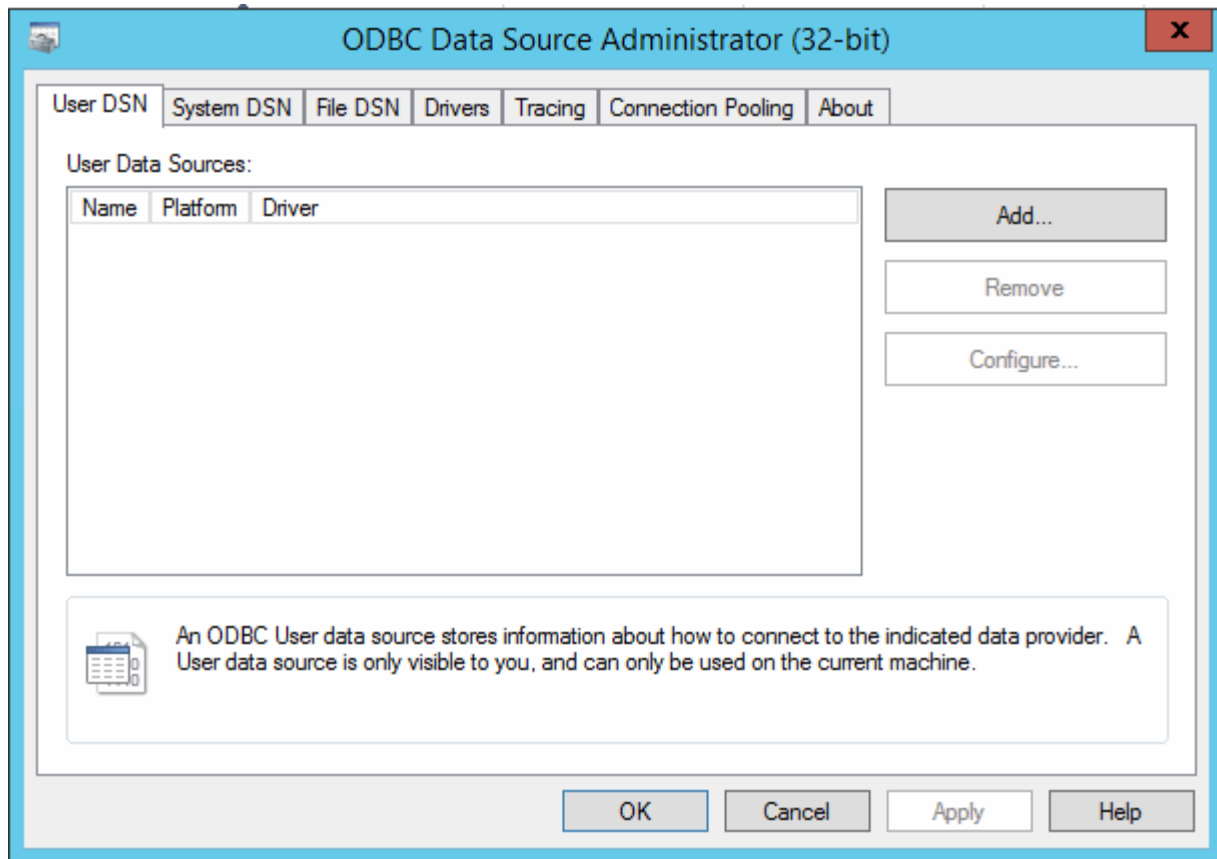
Antes de começar

Tem de efetuar um início de sessão remoto no servidor do Armazém de dados utilizando uma conta com o administrador Privileges.

Passos

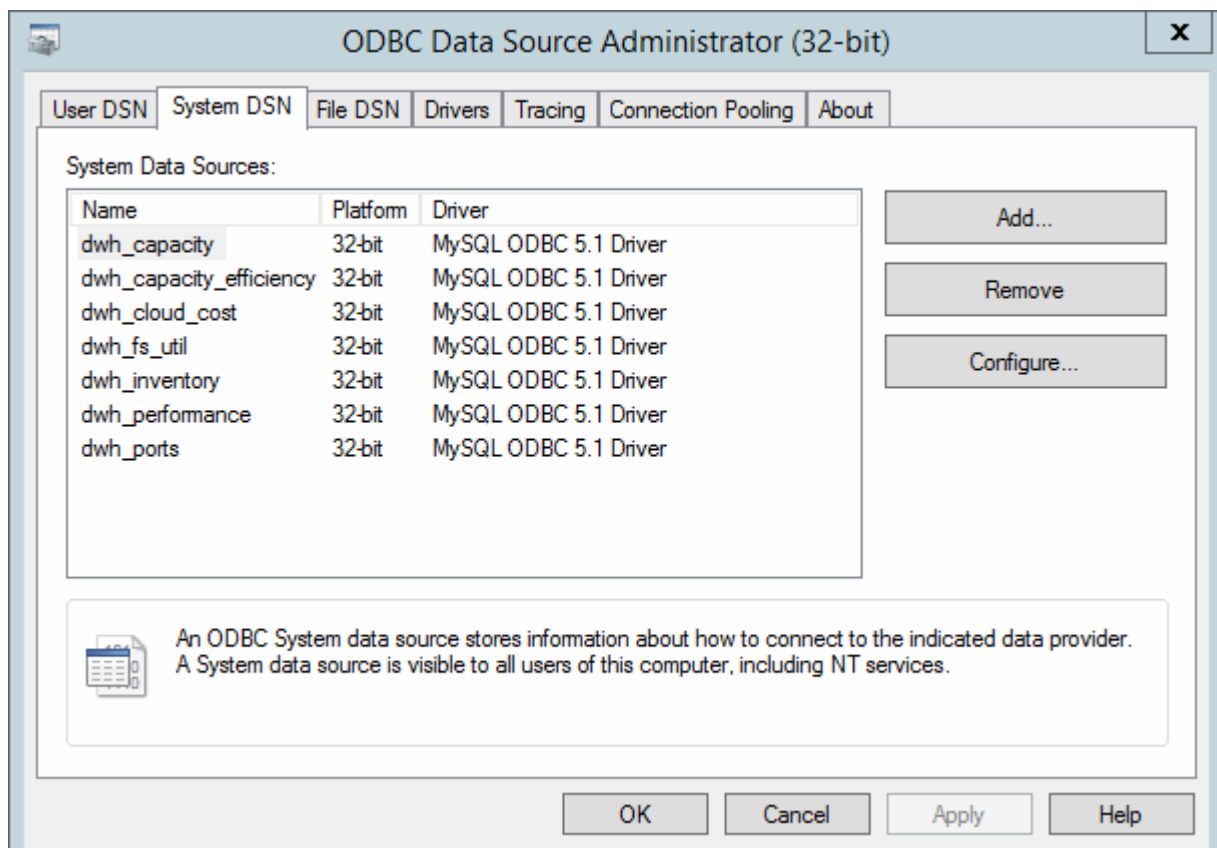
1. Faça um login remoto no servidor que hospeda esse Data Warehouse.
2. Acesse a ferramenta Administração ODBC em `C:\windows\SysWOW64\odbcad32.exe`

O sistema exhibe a tela Administrador da fonte de dados ODBC.



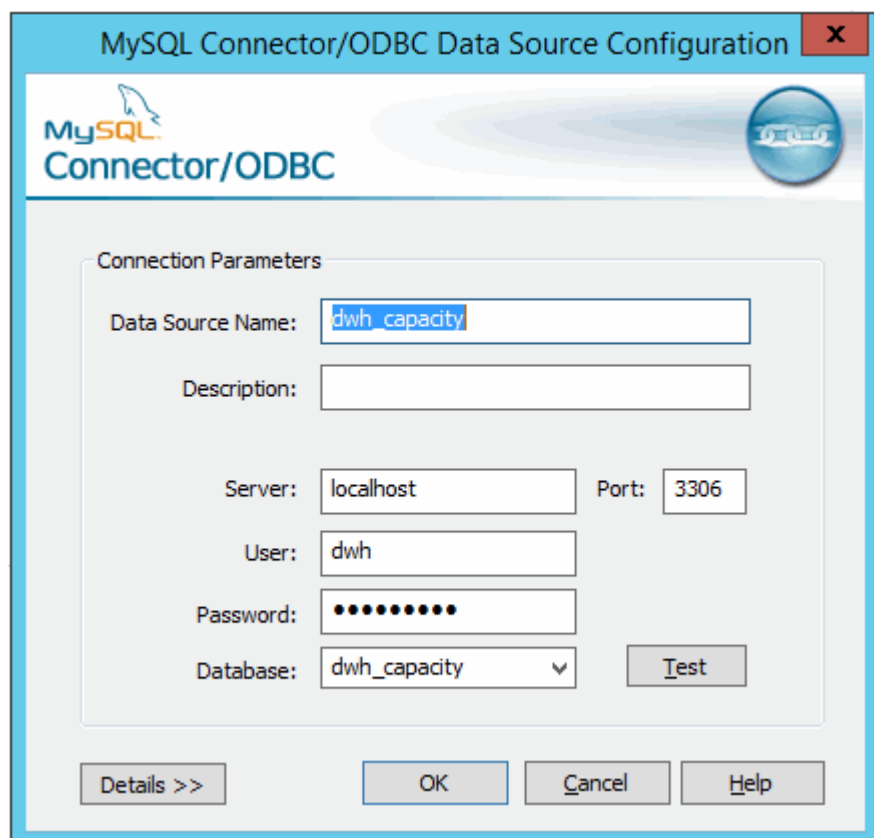
3. Clique em **System DSN**

São apresentadas as fontes de dados do sistema.



4. Selecione uma fonte de dados OnCommand Insight na lista.
5. Clique em **Configurar**

É apresentado o ecrã Data Source Configuration (Configuração da fonte de dados).



The image shows a screenshot of the 'MySQL Connector/ODBC Data Source Configuration' dialog box. The window title is 'MySQL Connector/ODBC Data Source Configuration' with a close button (X) in the top right corner. The dialog features the MySQL logo and 'Connector/ODBC' text on the left side. The main area is titled 'Connection Parameters' and contains several input fields: 'Data Source Name' (containing 'dwh_capacity'), 'Description' (empty), 'Server' (containing 'localhost'), 'Port' (containing '3306'), 'User' (containing 'dwh'), 'Password' (containing ten dots), and 'Database' (a dropdown menu showing 'dwh_capacity'). A 'Test' button is located to the right of the Database dropdown. At the bottom of the dialog, there are four buttons: 'Details >>', 'OK', 'Cancel', and 'Help'.

6. Introduza a nova palavra-passe no campo **Palavra-passe**.

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.