Seguridad y gestión de credenciales

SnapManager for SAP

NetApp
April 19, 2024

This PDF was generated from https://docs.netapp.com/es-es/snapmanager-sap/windows/concept-what-user-authentication-is.html on April 19, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Seguridad y gestión de credenciales

Puede gestionar la seguridad en SnapManager aplicando autenticación de usuario. El método de autenticación de usuario permite acceder a recursos como repositorios, hosts y perfiles.

Cuando se realiza una operación mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica de usuario (GUI), SnapManager recupera las credenciales establecidas para repositorios y perfiles. SnapManager guarda las credenciales de instalaciones anteriores.

El repositorio y los perfiles se pueden proteger con una contraseña. Una credencial es la contraseña configurada para el usuario de un objeto y la contraseña no está configurada en el objeto en sí.

Puede gestionar la autenticación y las credenciales realizando las siguientes tareas:

- Gestione la autenticación de usuario mediante solicitudes de contraseña en las operaciones o mediante el `smsap credential set` comando.

  Configurar credenciales para un repositorio, host o perfil.

- Vea las credenciales que rigen los recursos a los que tiene acceso.
- Borre las credenciales de un usuario para todos los recursos (hosts, repositorios y perfiles).
- Eliminar credenciales de un usuario para recursos individuales (hosts, repositorios y perfiles).

> Si la base de datos del repositorio está en un host de Windows, tanto el usuario local como el administrador y el usuario de dominio deben tener las mismas credenciales.

Qué es la autenticación de usuario

SnapManager autentica al usuario por medio de un inicio de sesión en el sistema operativo (SO) en el host en el que se ejecuta el servidor de SnapManager. Se puede habilitar la autenticación de usuario mediante solicitudes de contraseña en las operaciones o mediante la credencial de smo se puede habilitar la autenticación de usuarios a través de solicitudes de contraseña en las operaciones o mediante el uso de `smsap credential set`.

Los requisitos de autenticación de usuario dependen de dónde se realice la operación.

- Si el cliente SnapManager está en el mismo servidor que el host SnapManager, se autenticará mediante las credenciales del sistema operativo.

  No se le solicita una contraseña porque ya ha iniciado sesión en el host donde se ejecuta el servidor SnapManager.

- Si el cliente SnapManager y el servidor SnapManager están en hosts diferentes, SnapManager debe autenticarse con ambas credenciales de sistema operativo.

  SnapManager solicita contraseñas para cualquier operación si no se guardaron las credenciales del sistema operativo en la caché de credenciales del usuario SnapManager. Si introduce el `smsap credential set -host` Comando, puede guardar las credenciales del sistema operativo en su archivo

de caché de credenciales de SnapManager, por lo que SnapManager no solicita la contraseña de ninguna operación.

Si está autenticado con el servidor SnapManager, se considera el usuario efectivo. El usuario efectivo para cualquier operación debe ser una cuenta de usuario válida en el host donde se ejecuta la operación. Por ejemplo, si ejecuta una operación de clonado, debe poder iniciar sesión en el host de destino del clon.

SnapManager para SAP podría fallar al autorizar a los usuarios creados en Servicios de Active Directory central, como LDAP Y ANUNCIOS. Para asegurarse de que la autenticación no falla, debe configurar los valores configurables `auth.disableServerAuthorization` a **verdadero**.

Como usuario eficaz, puede gestionar las credenciales de las siguientes maneras:

- De manera opcional, es posible configurar SnapManager para almacenar credenciales de usuario en el archivo de credenciales de usuario de SnapManager.

  De manera predeterminada, SnapManager no almacena las credenciales del host. Puede resultar conveniente cambiar esto, por ejemplo, si tiene scripts personalizados que requieren acceso en un host remoto. La operación de clonado remoto es un ejemplo de una operación SnapManager que necesita las credenciales de inicio de sesión de un usuario para un host remoto. Para que SnapManager recuerde credenciales de inicio de sesión de host de usuario en la caché de credenciales de usuario de SnapManager, configure el `host.credentials.persist` propiedad para **true** en `smsap.config` archivo.

- Puede autorizar el acceso de los usuarios al repositorio.
- Puede autorizar el acceso de los usuarios a los perfiles.
- Es posible ver todas las credenciales de usuario.
- Es posible borrar las credenciales de un usuario para todos los recursos (hosts, repositorios y perfiles).
- Es posible eliminar credenciales de recursos individuales (hosts, repositorios y perfiles).

Almacenar contraseñas cifradas para scripts personalizados

De forma predeterminada, SnapManager no almacena credenciales de host en la caché de credenciales de usuario. Sin embargo, puede cambiar esto. Puede editar el `smsap.config` archivo para permitir el almacenamiento de credenciales de host.

Acerca de esta tarea

La `smsap.config` el archivo está ubicado en `<default installation location>\properties\smsap.config`

Pasos

1. Edite el `smsap.config` archivo.
2. Configurado *`host.credentials.persist`* a **verdadero**.

Autorizar el acceso al repositorio

SnapManager permite configurar credenciales para que los usuarios de la base de datos accedan al repositorio. Con las credenciales, puede restringir o evitar el acceso a hosts, repositorios, perfiles y bases de datos de SnapManager.

Acerca de esta tarea

Si establece las credenciales mediante el `credential set` SnapManager, no le solicita una contraseña.

Es posible configurar credenciales de usuario al instalar SnapManager o una versión posterior.

Paso

1. Introduzca el siguiente comando:

   smsap credential set -repository -dbname *repo_service_name* -host *repo_host* -login -username *repo_username* [-password *repo_password*] -port *repo_port*

Autorizar el acceso a los perfiles

SnapManager permite configurar una contraseña para un perfil para evitar el acceso no autorizado.

Paso

1. Introduzca el siguiente comando:

   smsap credential set -profile -name *profile_name* [-password *password*]

Ver las credenciales de usuario

Puede enumerar los hosts, perfiles y repositorios a los que tiene acceso.

Paso

1. Para enumerar los recursos a los que tiene acceso, escriba este comando:

   smsap credential list

Ejemplo de visualización de credenciales de usuario

En este ejemplo, se muestran los recursos a los que tiene acceso.

```
smsap credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMSAPREPO/hotspur:1521
Host2_test_user@SMSAPREPO/hotspur:1521
user1_1@SMSAPREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMSAPREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMSAPREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMSAPREPO/hotspur:1521) [PASSWORD NOT
SET]
Hosts:
Host2
Host5
```

Borrar credenciales de usuario para todos los hosts, repositorios y perfiles

Puede borrar la caché de sus credenciales para recursos (hosts, repositorios y perfiles). Esto elimina todas las credenciales de recursos del usuario que ejecuta el comando. Después de borrar la caché, debe volver a autenticar las credenciales para obtener acceso a estos recursos protegidos.

Pasos

1. Para borrar sus credenciales, introduzca el `smsap credential clear` Desde la CLI de SnapManager o seleccione **Admin** > **credenciales** > **Clear Cache** desde la GUI de SnapManager.
2. Salga de la interfaz gráfica de usuario de SnapManager.

   - Si borró la caché de credenciales de la interfaz gráfica de usuario de SnapManager, no es necesario salir de la interfaz gráfica de usuario de SnapManager.
   - Si borró la caché de credenciales de la interfaz de línea de comandos de SnapManager, debe reiniciar la interfaz gráfica de usuario de SnapManager.
   - Si ha eliminado manualmente el archivo de credenciales cifrado, deberá reiniciar de nuevo la interfaz gráfica de usuario de SnapManager.

3. Para volver a configurar las credenciales, repita el proceso con el fin de establecer las credenciales para el repositorio, el host del perfil y el perfil. Para obtener información adicional sobre cómo volver a configurar las credenciales de usuario, consulte "Configuración de credenciales tras borrar caché de credenciales".

Configure las credenciales después de borrar la caché de credenciales

Después de borrar la caché para quitar las credenciales de usuario almacenadas, puede configurar las credenciales para hosts, repositorios y perfiles.

Acerca de esta tarea

Debe asegurarse de establecer las mismas credenciales de usuario para el repositorio, el host del perfil y el perfil que había especificado anteriormente. Se crea un archivo de credenciales cifrado al configurar las credenciales de usuario.

El archivo de credenciales está ubicado en `C:\Documents and Settings\Administrator\Application Data\NetApp\smsap\3.3.0`.

Desde la interfaz gráfica de usuario (GUI) de SnapManager, si no hay ningún repositorio en repositorios, realice los siguientes pasos:

Pasos

1. Haga clic en **tareas** > **Agregar repositorio existente** para agregar un repositorio existente.
2. Ejecute los siguientes pasos para configurar las credenciales del repositorio:
   a. Haga clic con el botón derecho del ratón en el repositorio y seleccione **Abrir**.
   b. En la `Repository Credentials Authentication` introduzca las credenciales de usuario.
3. Realice los siguientes pasos para configurar las credenciales del host:
   a. Haga clic con el botón derecho del ratón en el host bajo el repositorio y seleccione **Abrir**.
   b. En la `Host Credentials Authentication` introduzca las credenciales de usuario.
4. Realice los siguientes pasos para configurar las credenciales del perfil:
   a. Haga clic con el botón derecho del ratón en el perfil bajo el host y seleccione **Abrir**.
   b. En la `Profile Credentials Authentication` introduzca las credenciales de usuario.

Eliminar credenciales de recursos individuales

Puede eliminar las credenciales de uno de los recursos protegidos, como un perfil, un repositorio o un host. De este modo, puede quitar las credenciales de un solo recurso, en lugar de borrar las credenciales del usuario de todos los recursos.

Eliminar credenciales de usuario para repositorios

Es posible eliminar las credenciales para que un usuario ya no pueda acceder a un repositorio en particular. Este comando permite quitar las credenciales de un solo recurso, en lugar de borrar las credenciales del usuario para todos los recursos.

Paso

1. Para eliminar credenciales de repositorio de un usuario, escriba este comando:

```
smsap credential delete -repository -dbname repo_service_name -host repo_host
-login -username repo_username -port repo_port
```

Eliminar credenciales de usuario para hosts

Es posible eliminar las credenciales de un host para que un usuario ya no pueda acceder a él. Este comando permite quitar las credenciales de un solo recurso, en lugar de borrar

todas las credenciales del usuario para todos los recursos.

Paso

1. Para eliminar credenciales de host de un usuario, escriba este comando:

```
smsap credential delete -host -name_host_name_-username_-username_
```

Eliminar credenciales de usuario para perfiles

Es posible eliminar las credenciales de usuario de un perfil para que un usuario ya no pueda acceder a él.

Paso

1. Para eliminar las credenciales de perfil de un usuario, escriba el siguiente comando:

```
smsap credential delete -profile -name profile_name
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.