Sicurezza e gestione delle credenziali

SnapManager for SAP

NetApp
April 19, 2024

Sommario

Sicurezza e gestione delle credenziali

È possibile gestire la sicurezza in SnapManager applicando l'autenticazione dell'utente. Il metodo di autenticazione dell'utente consente di accedere a risorse come repository, host e profili.

Quando si esegue un'operazione utilizzando l'interfaccia della riga di comando (CLI) o l'interfaccia utente grafica (GUI), SnapManager recupera il set di credenziali per repository e profili. SnapManager salva le credenziali delle installazioni precedenti.

Il repository e i profili possono essere protetti con una password. Una credenziale è la password configurata per l'utente per un oggetto e la password non è configurata sull'oggetto stesso.

È possibile gestire l'autenticazione e le credenziali eseguendo le seguenti operazioni:

- Gestire l'autenticazione dell'utente tramite richieste di password sulle operazioni o utilizzando `smsap credential set` comando.

  Impostare le credenziali per un repository, un host o un profilo.

- Visualizzare le credenziali che regolano le risorse a cui si ha accesso.
- Cancellare le credenziali di un utente per tutte le risorse (host, repository e profili).
- Eliminare le credenziali di un utente per le singole risorse (host, repository e profili).

Se il database del repository si trova su un host Windows, l'utente locale o amministratore e l'utente di dominio devono disporre delle stesse credenziali.

Che cos'è l'autenticazione dell'utente

SnapManager autentica l'utente utilizzando un accesso al sistema operativo (OS) sull'host in cui è in esecuzione il server SnapManager. È possibile attivare l'autenticazione dell'utente tramite la richiesta di password sulle operazioni o utilizzando la credenziale smo. È possibile attivare l'autenticazione dell'utente tramite la richiesta di password sulle operazioni o utilizzando `smsap credential set`.

I requisiti di autenticazione dell'utente dipendono da dove viene eseguita l'operazione.

- Se il client SnapManager si trova sullo stesso server dell'host SnapManager, l'utente viene autenticato dalle credenziali del sistema operativo.

  Non viene richiesta una password perché si è già connessi all'host in cui è in esecuzione il server SnapManager.

- Se il client SnapManager e il server SnapManager si trovano su host diversi, SnapManager deve autenticare l'utente con entrambe le credenziali del sistema operativo.

  Se non sono state salvate le credenziali del sistema operativo nella cache delle credenziali utente di SnapManager, SnapManager richiede le password per qualsiasi operazione. Se si immette `smsap credential set -host` Salvare le credenziali del sistema operativo nel file della cache delle credenziali di SnapManager, in modo che SnapManager non richieda la password per qualsiasi

operazione.

Se si è autenticati con il server SnapManager, si è considerati l'utente effettivo. L'utente effettivo per qualsiasi operazione deve essere un account utente valido sull'host su cui viene eseguita l'operazione. Ad esempio, se si esegue un'operazione di clonazione, dovrebbe essere possibile accedere all'host di destinazione per il clone.

SnapManager per SAP potrebbe non autorizzare gli utenti creati nei servizi Active Directory centrali, come LDAP e ADS. Per garantire che l'autenticazione non abbia esito negativo, è necessario impostare la configurazione `auth.disableServerAuthorization` a **true**.

In qualità di utente efficace, è possibile gestire le credenziali nei seguenti modi:

- In alternativa, è possibile configurare SnapManager in modo che memorizzi le credenziali utente nel file delle credenziali utente di SnapManager.

  Per impostazione predefinita, SnapManager non memorizza le credenziali host. Ad esempio, se si dispone di script personalizzati che richiedono l'accesso su un host remoto, è possibile modificare questa impostazione. L'operazione di clonazione remota è un esempio di un'operazione SnapManager che richiede le credenziali di accesso di un utente per un host remoto. Per fare in modo che SnapManager ricordi le credenziali di accesso dell'host utente nella cache delle credenziali utente di SnapManager, impostare `host.credentials.persist` proprietà a **true** in `smsap.config` file.

- È possibile autorizzare l'accesso dell'utente al repository.
- È possibile autorizzare l'accesso degli utenti ai profili.
- È possibile visualizzare tutte le credenziali utente.
- È possibile cancellare le credenziali di un utente per tutte le risorse (host, repository e profili).
- È possibile eliminare le credenziali per le singole risorse (host, repository e profili).

Memorizzare le password crittografate per gli script personalizzati

Per impostazione predefinita, SnapManager non memorizza le credenziali host nella cache delle credenziali utente. Tuttavia, è possibile modificare questa impostazione. È possibile modificare `smsap.config` file per consentire l'archiviazione delle credenziali host.

A proposito di questa attività

Il `smsap.config` il file si trova in `<default installation location>\properties\smsap.config`

Fasi

1. Modificare il `smsap.config` file.
2. Impostare *`host.credentials.persist`* a **true**.

Autorizzare l’accesso al repository

SnapManager consente di impostare le credenziali per consentire agli utenti del database di accedere al repository. Utilizzando le credenziali, è possibile limitare o impedire l’accesso agli host, ai repository, ai profili e ai database di SnapManager.

A proposito di questa attività

Se si impostano le credenziali utilizzando `credential set` SnapManager non richiede la password.

È possibile impostare le credenziali utente quando si installa SnapManager o versioni successive.

Fase

1. Immettere il seguente comando:

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

Autorizzare l’accesso ai profili

SnapManager consente di impostare una password per un profilo per impedire l’accesso non autorizzato.

Fase

1. Immettere il seguente comando:

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

Visualizzare le credenziali dell’utente

È possibile elencare gli host, i profili e i repository a cui si ha accesso.

Fase

1. Per elencare le risorse a cui si ha accesso, immettere questo comando:

   smsap credential list

Esempio di visualizzazione delle credenziali utente

In questo esempio vengono visualizzate le risorse a cui si dispone dell’accesso.

```
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
```

Cancella le credenziali utente per tutti gli host, i repository e i profili

È possibile cancellare la cache delle credenziali per le risorse (host, repository e profili). In questo modo vengono eliminate tutte le credenziali delle risorse per l'utente che esegue il comando. Dopo aver cancellato la cache, è necessario autenticare nuovamente le credenziali per accedere a queste risorse protette.

Fasi

1. Per cancellare le credenziali, immettere `smsap credential clear` Dalla CLI di SnapManager oppure selezionare **Amministratore** > **credenziali** > **Cancella cache** dalla GUI di SnapManager.
2. Uscire dalla GUI di SnapManager.

- Se la cache delle credenziali è stata cancellata dalla GUI di SnapManager, non è necessario uscire dalla GUI di SnapManager.
- Se la cache delle credenziali è stata cancellata dall'interfaccia utente di SnapManager, è necessario riavviare l'interfaccia utente di SnapManager.
- Se il file di credenziale crittografato è stato eliminato manualmente, è necessario riavviare nuovamente l'interfaccia grafica di SnapManager.

3. Per impostare nuovamente le credenziali, ripetere la procedura per impostare le credenziali per il repository, l'host del profilo e il profilo. Per ulteriori informazioni sulla nuova impostazione delle credenziali utente, fare riferimento a "impostazione delle credenziali dopo la cancellazione della cache delle credenziali".

Impostare le credenziali dopo aver cancellato la cache delle credenziali

Dopo aver cancellato la cache per rimuovere le credenziali utente memorizzate, è possibile impostare le credenziali per gli host, i repository e i profili.

A proposito di questa attività

È necessario assicurarsi di impostare le stesse credenziali utente per il repository, l'host del profilo e il profilo forniti in precedenza. Durante l'impostazione delle credenziali utente viene creato un file di credenziali crittografato.

Il file delle credenziali si trova in `C:\Documents and Settings\Administrator\Application Data\NetApp\smsap\3.3.0`.

Dall'interfaccia grafica utente (GUI) di SnapManager, se non è presente alcun repository in Repository, attenersi alla seguente procedura:

Fasi

1. Fare clic su **Tasks** > **Add Existing Repository** (Aggiungi repository esistente) per aggiungere un repository esistente.
2. Per impostare le credenziali per il repository, attenersi alla seguente procedura:
   a. Fare clic con il pulsante destro del mouse sul repository e selezionare **Apri**.
   b. In `Repository Credentials Authentication` immettere le credenziali dell'utente.
3. Per impostare le credenziali per l'host, attenersi alla seguente procedura:
   a. Fare clic con il pulsante destro del mouse sull'host sotto il repository e selezionare **Open** (Apri).
   b. In `Host Credentials Authentication` immettere le credenziali dell'utente.
4. Per impostare le credenziali per il profilo, procedere come segue:
   a. Fare clic con il pulsante destro del mouse sul profilo sotto l'host e selezionare **Open** (Apri).
   b. In `Profile Credentials Authentication` immettere le credenziali dell'utente.

Eliminare le credenziali per le singole risorse

È possibile eliminare le credenziali di una qualsiasi delle risorse protette, ad esempio un profilo, un repository o un host. In questo modo è possibile rimuovere le credenziali di una sola risorsa, invece di cancellare le credenziali dell'utente per tutte le risorse.

Eliminare le credenziali utente per i repository

È possibile eliminare le credenziali in modo che un utente non possa più accedere a un determinato repository. Questo comando consente di rimuovere le credenziali per una sola risorsa, invece di cancellare le credenziali dell'utente per tutte le risorse.

Fase

1. Per eliminare le credenziali del repository per un utente, immettere questo comando:

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

Eliminare le credenziali utente per gli host

È possibile eliminare le credenziali di un host in modo che un utente non possa più

accedervi. Questo comando consente di rimuovere le credenziali per una sola risorsa, invece di cancellare tutte le credenziali dell'utente per tutte le risorse.

Fase

1. Per eliminare le credenziali host per un utente, immettere il seguente comando:

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

Eliminare le credenziali utente per i profili

È possibile eliminare le credenziali utente per un profilo in modo che un utente non possa più accedervi.

Fase

1. Per eliminare le credenziali del profilo per un utente, immettere il seguente comando:

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