Funzionalità di sicurezza di SnapDrive per UNIX

Snapdrive for Unix

NetApp
October 04, 2023

Sommario

Funzionalità di sicurezza di SnapDrive per UNIX

Prima di utilizzare SnapDrive per UNIX, è necessario conoscerne le funzionalità di sicurezza e imparare ad accedervi.

Quali sono le funzioni di sicurezza

SnapDrive per UNIX offre alcune funzionalità che consentono di lavorare con esso in modo più sicuro. Queste funzionalità offrono un maggiore controllo su quali utenti possono eseguire operazioni su un sistema storage e da quale host.

Le funzioni di sicurezza consentono di eseguire le seguenti attività:

- Impostare le autorizzazioni per il controllo degli accessi
- Specificare le informazioni di accesso per i sistemi storage
- Specificare che SnapDrive per UNIX utilizza HTTPS

La funzione di controllo degli accessi consente di specificare le operazioni che un host che esegue SnapDrive per UNIX può eseguire su un sistema storage. Queste autorizzazioni vengono impostate singolarmente per ciascun host. Inoltre, per consentire a SnapDrive per UNIX di accedere a un sistema storage, è necessario fornire il nome di accesso e la password per tale sistema storage.

La funzione HTTPS consente di specificare la crittografia SSL per tutte le interazioni con il sistema di storage attraverso l'interfaccia Manage ONTAP (Gestione password), inclusa l'invio delle password. Questo comportamento è quello predefinito in SnapDrive 4.1 per UNIX e versioni successive per gli host AIX; tuttavia, è possibile disattivare la crittografia SSL modificando il valore di `use-https-to-filer` variabile di configurazione a. `off`.

Controllo degli accessi in SnapDrive per UNIX

SnapDrive per UNIX consente di controllare il livello di accesso di ciascun host a ciascun sistema storage a cui è connesso l'host.

Il livello di accesso in SnapDrive per UNIX indica le operazioni che l'host può eseguire quando si rivolge a un determinato sistema storage. Ad eccezione delle operazioni di visualizzazione ed elenco, le autorizzazioni per il controllo degli accessi possono influire su tutte le operazioni Snapshot e di storage.

Quali sono le impostazioni di controllo degli accessi

Per determinare l'accesso dell'utente, SnapDrive per UNIX controlla uno dei due file di permessi nel volume root del sistema di storage. Per valutare il controllo dell'accesso, è necessario controllare le regole impostate in tale file.

- `sdhost-name.prbac` il file si trova nella directory `/vol/vol0/sdprbac` (SnapDrive consente il controllo degli accessi basato sui ruoli).

  Il nome del file è `sdhost-name.prbac`, dove *`host-name`* è il nome dell'host a cui si applicano le autorizzazioni. È possibile disporre di un file di autorizzazioni per ciascun host collegato al sistema di storage. È possibile utilizzare `snapdrive config access` per visualizzare informazioni sulle

autorizzazioni disponibili per un host su un sistema storage specifico.

Se il `sdhost-name.prbac` non esiste, quindi utilizzare `sdgeneric.prbac` file per controllare le autorizzazioni di accesso.

- `sdgeneric.prbac` il file si trova anche nella directory `/vol/vol0/sdprbac`.

  Il nome del file `sdgeneric.prbac` viene utilizzato come impostazioni di accesso predefinite per più host a cui non è possibile accedere `sdhost-name.prbac` sul sistema storage.

Se avete entrambi `sdhost-name.prbac` e. `sdgeneric.prbac` file disponibili in `/vol/vol0/sdprbac` quindi utilizzare `sdhost-name.prbac` per controllare le autorizzazioni di accesso, in quanto sovrascrivono i valori forniti per `sdgeneric.prbac` file.

Se non si dispone di entrambe le opzioni `sdhost-name.prbac` e. `sdgeneric.prbac` quindi controllare la variabile di configurazione *`all-access-if-rbac-unspecified`* definito in `snapdrive.conf` file.

L'impostazione del controllo degli accessi da un host a una determinata unità vFiler è un'operazione manuale. L'accesso da un determinato host è controllato da un file che risiede nel volume root dell'unità vFiler interessata. Il file contiene `/vol/<vfiler root volume>/sdprbac/sdhost-name.prbac`, dove il *`host-name`* è il nome dell'host interessato, come restituito da `gethostname(3)`. Assicurarsi che il file sia leggibile, ma non scrivibile, dall'host che può accedervi.

> Per determinare il nome dell'host, eseguire `hostname` comando.

Se il file è vuoto, illeggibile o ha un formato non valido, SnapDrive per UNIX non concede all'host l'accesso a nessuna delle operazioni.

Se il file non è presente, SnapDrive per UNIX controlla la variabile di configurazione *`all-access-if-rbac-unspecified`* in `snapdrive.conf` file. Se la variabile è impostata su `on` (valore predefinito), consente agli host di accedere a tutte queste operazioni sul sistema storage. Se la variabile è impostata su `off`, SnapDrive per UNIX nega l'autorizzazione dell'host per eseguire qualsiasi operazione regolata dal controllo dell'accesso su tale sistema di storage.

Livelli di controllo degli accessi disponibili

SnapDrive per UNIX offre agli utenti diversi livelli di controllo degli accessi. Questi livelli di accesso sono correlati alle copie Snapshot e alle operazioni del sistema di storage.

È possibile impostare i seguenti livelli di accesso:

- NESSUNO — l'host non ha accesso al sistema di storage.
- CREAZIONE SNAP: L'host può creare copie Snapshot.
- UTILIZZO DI SNAP: L'host può eliminare e rinominare le copie Snapshot.
- SNAP ALL (SNAP TUTTO): L'host può creare, ripristinare, eliminare e rinominare le copie Snapshot.
- STORAGE CREATE DELETE (ELIMINA CREAZIONE STORAGE): L'host può creare, ridimensionare ed eliminare lo storage.
- UTILIZZO DELLO STORAGE: L'host può connettere e disconnettere lo storage ed eseguire anche la stima del clone split e l'avvio del clone split sullo storage.

- STORAGE ALL (TUTTO STORAGE): L'host può creare, eliminare, connettere e disconnettere lo storage ed eseguire anche la stima della divisione dei cloni e l'avvio della divisione dei cloni sullo storage.
- TUTTI GLI ACCESSI — l'host ha accesso a tutte le precedenti operazioni SnapDrive per UNIX.

Ogni livello è distinto. Se si specifica l'autorizzazione solo per determinate operazioni, SnapDrive per UNIX può eseguire solo tali operazioni. Ad esempio, se si specifica L'UTILIZZO DELLO STORAGE, l'host può utilizzare SnapDrive per UNIX per connettere e disconnettere lo storage, ma non può eseguire altre operazioni governate dalle autorizzazioni di controllo degli accessi.

Impostazione dell'autorizzazione per il controllo degli accessi

È possibile impostare l'autorizzazione per il controllo degli accessi in SnapDrive per UNIX creando una directory e un file speciali nel volume root del sistema di storage.

Assicurarsi di aver effettuato l'accesso come utente root.

Fasi

1. Creare la directory `sdprbac` nel volume root del sistema storage di destinazione.

   Un modo per rendere accessibile il volume root è montare il volume utilizzando NFS.

2. Creare il file delle autorizzazioni in `sdprbac` directory. Assicurarsi che le seguenti affermazioni siano vere:

   - Il file deve essere denominato `sdhost-name.prbac` dove host-name è il nome dell'host per cui si specificano le autorizzazioni di accesso.
   - Il file deve essere di sola lettura per garantire che SnapDrive per UNIX possa leggerlo, ma che non possa essere modificato.

     Per assegnare a un host il permesso di accesso dev-sun1, creare il seguente file sul sistema storage: `/vol/vol1/sdprbac/sddev-sun1.prbac`

3. Impostare le autorizzazioni nel file per l'host.

   Per il file è necessario utilizzare il seguente formato:

   - È possibile specificare un solo livello di autorizzazioni. Per fornire all'host l'accesso completo a tutte le operazioni, inserire la stringa ALL ACCESS.
   - La stringa di autorizzazione deve essere la prima cosa nel file. Il formato del file non è valido se la stringa di autorizzazione non si trova nella prima riga.
   - Le stringhe di permesso non distinguono tra maiuscole e minuscole.
   - Nessuno spazio vuoto può precedere la stringa di permesso.
   - Non sono consentiti commenti.

     Queste stringhe di autorizzazione valide consentono i seguenti livelli di accesso:

   - NESSUNO — l'host non ha accesso al sistema di storage.
   - CREAZIONE SNAP: L'host può creare copie Snapshot.
   - UTILIZZO DI SNAP: L'host può eliminare e rinominare le copie Snapshot.
   - SNAP ALL (SNAP TUTTO): L'host può creare, ripristinare, eliminare e rinominare le copie Snapshot.

- STORAGE CREATE DELETE (ELIMINA CREAZIONE STORAGE): L'host può creare, ridimensionare ed eliminare lo storage.
- UTILIZZO DELLO STORAGE: L'host può connettere e disconnettere lo storage ed eseguire anche la stima del clone split e l'avvio del clone split sullo storage.
- STORAGE ALL (TUTTO STORAGE): L'host può creare, eliminare, connettere e disconnettere lo storage ed eseguire anche la stima della divisione dei cloni e l'avvio della divisione dei cloni sullo storage.
- TUTTI GLI ACCESSI — l'host ha accesso a tutte le precedenti operazioni SnapDrive per UNIX. Ciascuna di queste stringhe di autorizzazione è discreta. Se si specifica L'UTILIZZO DELLO SNAP, l'host può eliminare o rinominare le copie Snapshot, ma non può creare copie Snapshot o ripristinare o eseguire operazioni di provisioning dello storage.

Indipendentemente dalle autorizzazioni impostate, l'host può eseguire operazioni di visualizzazione ed elenco.

4. Verificare le autorizzazioni di accesso immettendo il seguente comando:

   `snapdrive config access show` *`filer_name`*

Visualizzazione dell'autorizzazione per il controllo degli accessi

È possibile visualizzare le autorizzazioni per il controllo degli accessi eseguendo `snapdrive config access show` comando.

Fasi

1. Eseguire `snapdrive config access show` comando.

   Questo comando ha il seguente formato: `snapdrive config access {show | list} filename`

   È possibile utilizzare gli stessi parametri indipendentemente dall'immissione o meno di `show` oppure `list` versione del comando.

   Questa riga di comando controlla il tostapane del sistema di storage per determinare le autorizzazioni di cui dispone l'host. In base all'output, le autorizzazioni per l'host su questo sistema di storage sono SNAP-ALL.

   ```
   # snapdrive config access show toaster
   This host has the following access permission to filer, toaster:
   SNAP ALL
   Commands allowed:
   snap create
   snap restore
   snap delete
   snap rename
   #
   ```

   In questo esempio, il file delle autorizzazioni non si trova sul sistema di storage, quindi SnapDrive per UNIX controlla la variabile *`all-access-if-rbac-unspecified`* in `snapdrive.conf` file per determinare le autorizzazioni di cui dispone l'host. Questa variabile è impostata su on, che equivale alla

creazione di un file di permessi con il livello di accesso impostato su TUTTI GLI ACCESSI.

```
# snapdrive config access list toaster
This host has the following access permission to filer, toaster:
ALL ACCESS
Commands allowed:
snap create
snap restore
snap delete
snap rename
storage create
storage resize
snap connect
storage connect
storage delete
snap disconnect
storage disconnect
clone split estimate
clone split start
#
```

Questo esempio mostra il tipo di messaggio ricevuto se non è presente alcun file di permessi sul tostapane del sistema di storage e la variabile *`all-access-if-rbac-unspecified`* in `snapdrive.conf` il file è impostato su `off`.

```
# snapdrive config access list toaster
Unable to read the access permission file on filer, toaster. Verify that
the
file is present.
Granting no permissions to filer, toaster.
```

Informazioni di accesso per i sistemi storage

Un nome utente o una password consentono a SnapDrive per UNIX di accedere a ciascun sistema di storage. Fornisce inoltre sicurezza perché, oltre ad essere connesso come root, la persona che esegue SnapDrive per UNIX deve fornire il nome utente o la password corretti quando richiesto. Se un accesso viene compromesso, è possibile eliminarlo e impostare un nuovo accesso utente.

È stato creato il login utente per ciascun sistema storage al momento della configurazione. Affinché SnapDrive per UNIX funzioni con il sistema di storage, è necessario fornire queste informazioni di accesso. A seconda di quanto specificato al momento della configurazione dei sistemi storage, ciascun sistema storage potrebbe utilizzare lo stesso login o un login univoco.

SnapDrive per UNIX memorizza questi login e password in forma crittografata su ciascun host. È possibile

specificare che SnapDrive per UNIX crittografi queste informazioni quando comunicano con il sistema di storage impostando *snapdrive.conf* variabile di configurazione *use-https-to-filer=on*.

Specifica delle informazioni di accesso

È necessario specificare le informazioni di accesso utente per un sistema di storage. A seconda di quanto specificato al momento della configurazione del sistema di storage, ciascun sistema di storage potrebbe utilizzare lo stesso nome utente o password oppure un nome utente o una password univoci. Se tutti i sistemi di storage utilizzano le stesse informazioni relative al nome utente o alla password, è necessario eseguire una sola volta le seguenti operazioni. Se i sistemi di storage utilizzano nomi utente o password univoci, è necessario ripetere la procedura seguente per ciascun sistema di storage.

Assicurarsi di aver effettuato l'accesso come utente root.

Fasi

1. Immettere il seguente comando:

   snapdrive config set *user_name filename* [*filename*…]

   user_name è il nome utente specificato per il sistema di storage al momento della prima configurazione.

   filename è il nome del sistema di storage.

   [filename…] definisce che è possibile inserire più nomi di sistemi di storage su una riga di comando se tutti hanno lo stesso nome utente o password. Immettere il nome di almeno un sistema storage.

2. Quando richiesto, inserire la password, se presente.

   > Se non è stata impostata alcuna password, premere Invio (il valore nullo) quando viene richiesta una password.

   In questo esempio viene impostato un utente chiamato `root` per un sistema di storage chiamato toaster:

   ```
   # snapdrive config set `root` toaster
   Password for root:
   Retype Password:
   ```

   In questo esempio viene impostato un utente chiamato `root` per tre sistemi storage:

   ```
   # snapdrive config set root toaster oven broiler
   Password for root:
   Retype Password:
   ```

3. Se si dispone di un altro sistema di storage con un nome utente o una password diversi, ripetere la procedura.

Verifica dei nomi utente del sistema di storage associati a SnapDrive per UNIX

È possibile verificare quale nome utente SnapDrive per UNIX è associato a un sistema di storage eseguendo `snapdrive config list` comando.

È necessario aver effettuato l'accesso come utente root.

Fasi

1. Immettere il seguente comando:

   `snapdrive config list`

   Questo comando visualizza il nome utente o le coppie di sistemi di storage per tutti i sistemi che hanno utenti specificati in SnapDrive per UNIX. Non vengono visualizzate le password dei sistemi di storage.

   Questo esempio mostra gli utenti associati ai sistemi storage denominati rapunzel e sistema storage medio:

   ```
   # snapdrive config list
   user name           storage system name
   ----------------------------
   rumplestiltskins    rapunzel
   longuser            mediumstoragesystem
   ```

Eliminazione di un login utente per un sistema storage

È possibile eliminare un accesso utente per uno o più sistemi storage eseguendo `snapdrive config delete` comando.

Assicurarsi di aver effettuato l'accesso come utente root.

Fasi

1. Immettere il seguente comando:

   `snapdrive config delete` *`appliance_name [appliance_name]`*

   `appliance_name` è il nome del sistema di storage per il quale si desidera eliminare le informazioni di accesso dell'utente.

   SnapDrive per UNIX rimuove le informazioni di accesso relative al nome utente o alla password per i sistemi di storage specificati.

   > Per consentire a SnapDrive per UNIX di accedere al sistema di storage, è necessario specificare un nuovo login utente.

Impostazione di HTTP

È possibile configurare SnapDrive per UNIX in modo che utilizzi HTTP per la piattaforma

host.

Assicurarsi di aver effettuato l'accesso come utente root.

Fasi

1. Eseguire un backup di `snapdrive.conf` file.
2. Aprire `snapdrive.conf` in un editor di testo.
3. Modificare il valore di *`use-https-to-filer`* variabile a. `off`.

   Una buona pratica ogni volta che si modifica `snapdrive.conf` il file deve eseguire le seguenti operazioni:

   a. Commentare la riga che si desidera modificare.
   b. Copia la riga commentata.
   c. Rimuovere il commento dal testo copiato rimuovendo il simbolo cancelletto.
   d. Modificare il valore.
4. Salvare il file dopo aver apportato le modifiche.

   SnapDrive per UNIX controlla automaticamente questo file ogni volta che viene avviato. Per rendere effettive le modifiche, riavviare il daemon SnapDrive per UNIX.