Sicherheitsfunktionen in SnapDrive für UNIX

Snapdrive for Unix

NetApp
June 20, 2025

Inhalt

Sicherheitsfunktionen in SnapDrive für UNIX

Bevor Sie SnapDrive für UNIX verwenden, müssen Sie seine Sicherheitsfunktionen kennen und lernen, wie Sie darauf zugreifen können.

Was sind die Sicherheitsfunktionen

SnapDrive für UNIX bietet bestimmte Funktionen, die eine sicherere Arbeit ermöglichen. Diese Funktionen bieten Ihnen mehr Kontrolle darüber, welche Benutzer Vorgänge auf einem Storage-System ausführen können und von welchem Host aus.

Mit den Sicherheitsfunktionen können Sie die folgenden Aufgaben ausführen:

- Zugriffskontrollberechtigungen einrichten
- Geben Sie Anmeldeinformationen für die Storage-Systeme an
- Geben Sie an, dass SnapDrive für UNIX HTTPS verwenden soll

Über die Zugriffskontrollfunktion können Sie festlegen, welche Vorgänge ein Host, auf dem SnapDrive für UNIX ausgeführt wird, auf einem Speichersystem ausführen kann. Sie legen diese Berechtigungen für jeden Host individuell fest. Darüber hinaus müssen Sie für SnapDrive für UNIX den Zugriff auf ein Speichersystem zulassen, dass Sie den Anmeldenamen und das Passwort für dieses Speichersystem angeben.

Mit der HTTPS-Funktion können Sie die SSL-Verschlüsselung für alle Interaktionen mit dem Speichersystem über die ONTAP-Schnittstelle verwalten angeben, einschließlich des Versands der Passwörter. Dieses Verhalten ist die Standardeinstellung in SnapDrive 4.1 für UNIX und neuere Versionen für AIX-Hosts. Sie können jedoch die SSL-Verschlüsselung deaktivieren, indem Sie den Wert der ändern `use-https-to-filer` Konfigurationsvariable auf `off`.

Zugriffssteuerung in SnapDrive für UNIX

Mit SnapDrive für UNIX können Sie die Zugriffsebene kontrollieren, die jeder Host für jedes Storage-System hat, mit dem der Host verbunden ist.

Die Zugriffsebene in SnapDrive für UNIX gibt an, welche Vorgänge der Host ausführen darf, wenn er auf ein bestimmtes Speichersystem ausgerichtet ist. Mit Ausnahme der Show- und Listenvorgänge können sich die Berechtigungen für die Zugriffssteuerung auf alle Snapshot- und Storage-Vorgänge auswirken.

Welche Zugriffskontrolleinstellungen sind

Um den Benutzerzugriff zu bestimmen, überprüft SnapDrive für UNIX eine von zwei Berechtigungsdateien im Root-Volume des Speichersystems. Sie müssen die in dieser Datei festgelegten Regeln überprüfen, um die Zugriffssteuerung zu bewerten.

- `sdhost-name.prbac` Die Datei befindet sich im Verzeichnis `/vol/vol0/sdprbac` (SnapDrive Berechtigungen rollenbasierte Zugriffssteuerung).

  Der Dateiname lautet `sdhost-name.prbac`, Wo *`host-name`* Ist der Name des Hosts, auf den die Berechtigungen gelten. Sie können für jeden Host, der mit dem Speichersystem verbunden ist, eine Berechtigungsdatei haben. Sie können das verwenden `snapdrive config access` Befehl zum

Anzeigen von Informationen über die für einen Host verfügbaren Berechtigungen auf einem bestimmten Speichersystem.

Wenn der `sdhost-name.prbac` Ist nicht vorhanden, verwenden Sie dann das `sdgeneric.prbac` Datei, um die Zugriffsberechtigungen zu prüfen.

- `sdgeneric.prbac` Datei ist auch im Verzeichnis `/vol/vol0/sdprbac`.

  Der Dateiname `sdgeneric.prbac` Wird als Standard-Zugriffseinstellungen für mehrere Hosts verwendet, die keinen Zugriff auf haben `sdhost-name.prbac` Datei auf dem Speichersystem.

Wenn Sie beides haben `sdhost-name.prbac` Und `sdgeneric.prbac` Dateien, die im verfügbar sind `/vol/vol0/sdprbac` Verwenden Sie dann den Pfad `sdhost-name.prbac` Um die Zugriffsberechtigungen zu überprüfen, werden die Werte, für die sie bereitgestellt wurden, überschrieben `sdgeneric.prbac` Datei:

Wenn Sie nicht beide haben `sdhost-name.prbac` Und `sdgeneric.prbac` Dateien und anschließend die Konfigurationsvariable prüfen *`all-access-if-rbac-unspecified`* Das wird im definiert `snapdrive.conf` Datei:

Die Einrichtung der Zugriffssteuerung von einem bestimmten Host zu einer bestimmten vFiler Einheit erfolgt manuell. Der Zugriff von einem bestimmten Host wird durch eine Datei im Root-Volume der betroffenen vFiler Einheit gesteuert. Die Datei enthält `/vol/<vfiler root volume>/sdprbac/sdhost-name.prbac`, Wo der *`host-name`* Ist der Name des betroffenen Hosts, der von zurückgegeben wird `gethostname(3)`. Sie sollten sicherstellen, dass diese Datei vom Host, der auf sie zugreifen kann, lesbar, aber nicht beschreibbar ist.

Um den Namen des Hosts zu bestimmen, führen Sie den aus `hostname` Befehl.

Wenn die Datei leer, unlesbar oder ein ungültiges Format hat, gewährt SnapDrive für UNIX dem Host keinen Zugriff auf die Vorgänge.

Wenn die Datei fehlt, überprüft SnapDrive für UNIX die Konfigurationsvariable *`all-access-if-rbac-unspecified`* Im `snapdrive.conf` Datei: Wenn die Variable auf festgelegt ist `on` (Standardwert). Sie ermöglicht den Hosts vollständigen Zugriff auf all diese Vorgänge auf diesem Speichersystem. Wenn die Variable auf festgelegt ist `off`, SnapDrive für UNIX verweigert die Host-Berechtigung, alle Operationen durchzuführen, die durch die Zugriffssteuerung auf diesem Speichersystem geregelt sind.

Verfügbare Zugriffssteuerungsstufen

SnapDrive für UNIX bietet Benutzern verschiedene Zugriffskontrollebenen. Diese Zugriffsebenen beziehen sich auf die Snapshot Kopien und die Storage-Systemvorgänge.

Sie können die folgenden Zugriffsebenen festlegen:

- KEINE – der Host hat keinen Zugriff auf das Speichersystem.
- SNAP ERSTELLEN – der Host kann Snapshot Kopien erstellen.
- SNAP USE – der Host kann Snapshot Kopien löschen und umbenennen.
- SNAP ALL – der Host kann Snapshot Kopien erstellen, wiederherstellen, löschen und umbenennen.
- STORAGE CREATE DELETE - der Host kann Speicher erstellen, anpassen und löschen.
- STORAGE-NUTZUNG – der Host kann eine Verbindung zum Storage herstellen und die Verbindung trennen. Außerdem lassen sich Aufteilungen von Klonen und Split beginnen auf dem Storage.

- GESAMTER STORAGE – der Host kann Storage erstellen, löschen, verbinden und trennen. Außerdem kann er die Klonteilschätzung und den Start der Klonteilteilung auf dem Storage vornehmen.
- ZUGRIFF – der Host hat Zugriff auf alle zuvor genannten SnapDrive für UNIX-Vorgänge.

Jede Ebene ist klar. Wenn Sie nur für bestimmte Vorgänge die Berechtigung angeben, kann SnapDrive für UNIX nur die Vorgänge ausführen. Wenn Sie BEISPIELSWEISE SPEICHER VERWENDEN angeben, kann der Host SnapDrive für UNIX zum Verbinden und Trennen von Speicher verwenden. Andere Vorgänge, die durch Zugriffskontrollberechtigungen geregelt sind, können jedoch nicht ausgeführt werden.

Einrichten der Zugriffskontrollberechtigung

Sie können Zugriffskontrollrechte in SnapDrive für UNIX einrichten, indem Sie ein spezielles Verzeichnis und eine Datei im Root-Volume des Speichersystems erstellen.

Stellen Sie sicher, dass Sie als Root-Benutzer angemeldet sind.

Schritte

1. Erstellen Sie das Verzeichnis `sdprbac` Im Root-Volume des Ziel-Storage-Systems.

   Eine Möglichkeit, auf das Root-Volume zugreifen zu können, ist das Mounten des Volumes mit NFS.

2. Erstellen Sie die Berechtigungsdatei im `sdprbac` Verzeichnis. Stellen Sie sicher, dass die folgenden Aussagen richtig sind:
   - Die Datei muss benannt sein `sdhost-name.prbac` Dabei ist der Hostname der Name des Hosts, für den Sie die Zugriffsberechtigungen angeben.
   - Die Datei muss schreibgeschützt sein, um sicherzustellen, dass SnapDrive für UNIX sie lesen kann, aber dass sie nicht geändert werden kann.

     Um einem Host namens „dev-sun1“ Zugriff zu gewähren, würden Sie folgende Datei auf dem Storage-System erstellen: `/vol/vol1/sdprbac/sddev-sun1.prbac`

3. Legen Sie die Berechtigungen in der Datei für diesen Host fest.

   Sie müssen das folgende Format für die Datei verwenden:

   - Sie können nur eine Berechtigungsstufe angeben. Um dem Host vollständigen Zugriff auf alle Vorgänge zu geben, geben Sie die Zeichenfolge ALLEN ZUGRIFF ein.
   - Die Berechtigungszeichenfolge muss das erste in der Datei sein. Das Dateiformat ist ungültig, wenn sich die Berechtigungszeichenfolge nicht in der ersten Zeile befindet.
   - Die Groß-/Kleinschreibung von Berechtigungs-Strings wird nicht berücksichtigt.
   - Kein Leerzeichen kann vor der Berechtigungszeichenfolge liegen.
   - Keine Kommentare sind erlaubt.

     Diese gültigen Berechtigungs-Strings ermöglichen die folgenden Zugriffsebenen:

   - KEINE – der Host hat keinen Zugriff auf das Speichersystem.
   - SNAP ERSTELLEN – der Host kann Snapshot Kopien erstellen.
   - SNAP USE – der Host kann Snapshot Kopien löschen und umbenennen.
   - SNAP ALL – der Host kann Snapshot Kopien erstellen, wiederherstellen, löschen und umbenennen.

- STORAGE CREATE DELETE - der Host kann Speicher erstellen, anpassen und löschen.
- STORAGE-NUTZUNG – der Host kann eine Verbindung zum Storage herstellen und die Verbindung trennen. Außerdem lassen sich Aufteilungen von Klonen und Split beginnen auf dem Storage.
- GESAMTER STORAGE – der Host kann Storage erstellen, löschen, verbinden und trennen. Außerdem kann er die Klonteilschätzung und den Start der Klonteilteilung auf dem Storage vornehmen.
- ZUGRIFF – der Host hat Zugriff auf alle zuvor genannten SnapDrive für UNIX-Vorgänge. Jeder dieser Berechtigungs-Strings ist diskret. Wenn Sie SNAP USE angeben, kann der Host Snapshot Kopien löschen oder umbenennen, dies kann aber keine Snapshot Kopien oder Restores erstellen oder Storage-Bereitstellungsvorgänge ausführen.

Unabhängig von den festgelegten Berechtigungen kann der Host Anzeigen- und Listenvorgänge durchführen.

4. Überprüfen Sie die Zugriffsberechtigungen, indem Sie den folgenden Befehl eingeben:

   `snapdrive config access show filer_name`

Zugriffsberechtigung anzeigen

Sie können die Zugriffskontrollberechtigungen anzeigen, indem Sie das ausführen `snapdrive config access show` Befehl.

Schritte

1. Führen Sie die aus `snapdrive config access show` Befehl.

   Dieser Befehl weist das folgende Format auf: `snapdrive config access {show | list} filername`

   Sie können die gleichen Parameter verwenden, unabhängig davon, ob Sie den eingeben `show` Oder `list` Version des Befehls.

   Diese Befehlszeile überprüft den Toaster des Speichersystems, um festzustellen, welche Berechtigungen der Host hat. Basierend auf der Ausgabe sind die Berechtigungen für den Host auf diesem Speichersystem 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 diesem Beispiel befindet sich die Berechtigungsdatei nicht auf dem Speichersystem, daher überprüft SnapDrive für UNIX die Variable *`all-access-if-rbac-unspecified`* Im `snapdrive.conf` Datei, um zu bestimmen, welche Berechtigungen der Host besitzt. Diese Variable wird auf ein gesetzt, was der

Erstellung einer Berechtigungsdatei entspricht, deren Zugriffsebene für ALLE ZUGRIFFE festgelegt ist.

```
# 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
#
```

Dieses Beispiel zeigt die Art der Meldung, die Sie erhalten, wenn sich keine Berechtigungsdatei auf dem Speichersystem Toaster befindet, und die Variable *`all-access-if-rbac-unspecified`* Im `snapdrive.conf` Datei ist auf festgelegt `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.
```

Anmeldeinformationen für Storage-Systeme

Ein Benutzername oder Passwort ermöglicht SnapDrive für UNIX den Zugriff auf jedes Speichersystem. Es bietet auch Sicherheit, weil die Person, die SnapDrive für UNIX ausführt, neben der Anmeldung als root den korrekten Benutzernamen oder das richtige Passwort angeben muss, wenn sie dazu aufgefordert wird. Wenn eine Anmeldung kompromittiert ist, können Sie sie löschen und einen neuen Benutzer anmelden.

Sie haben bei Ihrer Einrichtung die Benutzer-Anmeldung für die einzelnen Storage-Systeme erstellt. Damit SnapDrive für UNIX mit dem Speichersystem arbeiten kann, müssen Sie diese Anmeldedaten angeben. Je nachdem, was Sie beim Einrichten der Storage-Systeme angegeben haben, kann jedes Storage-System entweder dieselbe Anmeldung oder eine eindeutige Anmeldung verwenden.

SnapDrive für UNIX speichert diese Anmeldungen und Passwörter in verschlüsselter Form auf jedem Host. Sie

können angeben, dass SnapDrive für UNIX diese Informationen verschlüsseln, wenn sie mit dem Speichersystem kommunizieren, indem Sie auf setzen *snapdrive.conf* Konfigurationsvariable *use-https-to-filer=on*.

Angeben von Anmeldeinformationen

Sie müssen die Anmeldeinformationen des Benutzers für ein Speichersystem angeben. Je nachdem, was Sie beim Einrichten des Storage-Systems angegeben haben, kann jedes Storage-System entweder denselben Benutzernamen oder dasselbe Passwort oder einen eindeutigen Benutzernamen oder ein Kennwort verwenden. Wenn alle Speichersysteme denselben Benutzernamen oder dieselben Kennwortinformationen verwenden, müssen Sie die folgenden Schritte einmal ausführen. Wenn die Speichersysteme eindeutige Benutzernamen oder Passwörter verwenden, müssen Sie die folgenden Schritte für jedes Speichersystem wiederholen.

Stellen Sie sicher, dass Sie als Root-Benutzer angemeldet sind.

Schritte

1. Geben Sie den folgenden Befehl ein:

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

   user_name Ist der Benutzername, der beim ersten Einrichten für dieses Storage-System angegeben wurde.

   filername Ist der Name des Storage-Systems.

   [filername…] Definiert, dass Sie mehrere Storage-Systemnamen in einer Befehlszeile eingeben können, wenn alle über dasselbe Benutzeranmeldung oder Passwort verfügen. Sie müssen den Namen von mindestens einem Storage-System eingeben.

2. Geben Sie an der Eingabeaufforderung das Passwort ein, wenn vorhanden.

   Wenn kein Passwort festgelegt wurde, drücken Sie die Eingabetaste (der Null-Wert), wenn Sie zur Eingabe eines Passworts aufgefordert werden.

   In diesem Beispiel wird ein Benutzer mit dem Namen eingerichtet `root` Für ein Speichersystem namens Toaster:

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

   In diesem Beispiel wird ein Benutzer mit dem Namen eingerichtet `root` Für drei Storage-Systeme:

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

3. Wenn Sie ein anderes Speichersystem mit einem anderen Benutzernamen oder einem anderen Kennwort haben, wiederholen Sie diese Schritte.

Überprüfung der mit SnapDrive für UNIX verknüpften Benutzernamen auf Storage-Systemen

Sie können überprüfen, welcher Benutzername SnapDrive für UNIX mit einem Speichersystem verbunden ist, indem Sie die ausführen `snapdrive config list` Befehl.

Sie müssen sich als Root-Benutzer angemeldet haben.

Schritte

1. Geben Sie den folgenden Befehl ein:

   `snapdrive config list`

   Mit diesem Befehl werden der Benutzername oder die Speichersystempaare für alle Systeme angezeigt, auf denen Benutzer in SnapDrive für UNIX angegeben sind. Die Passwörter für die Speichersysteme werden nicht angezeigt.

   In diesem Beispiel werden die Benutzer angezeigt, die mit den Storage-Systemen namens rapunzel und dem mittelgroßen Storage-System verbunden sind:

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

Löschen einer Benutzeranmeldung für ein Speichersystem

Sie können eine Benutzeranmeldung für ein oder mehrere Speichersysteme löschen, indem Sie die ausführen `snapdrive config delete` Befehl.

Stellen Sie sicher, dass Sie als Root-Benutzer angemeldet sind.

Schritte

1. Geben Sie den folgenden Befehl ein:

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

   `appliance_name` Ist der Name des Speichersystems, für das Sie die Benutzeranmeldedaten löschen

möchten.

SnapDrive für UNIX entfernt den Benutzernamen oder die Passwort-Anmeldeinformationen für die von Ihnen angegebenen Speichersysteme.

Um SnapDrive für UNIX für den Zugriff auf das Speichersystem zu aktivieren, müssen Sie eine neue Benutzeranmeldung angeben.

Einrichten von HTTP

Sie können SnapDrive für UNIX so konfigurieren, dass HTTP für Ihre Host-Plattform verwendet wird.

Stellen Sie sicher, dass Sie als Root-Benutzer angemeldet sind.

Schritte

1. Erstellen Sie ein Backup der `snapdrive.conf` Datei:
2. Öffnen Sie das `snapdrive.conf` Datei in einem Texteditor.
3. Ändern Sie den Wert des *`use-https-to-filer`* Variabel auf `off`.

   Eine gute Praxis, jedes Mal, wenn Sie die ändern `snapdrive.conf` Die Datei führt die folgenden Schritte aus:

   a. Kommentieren Sie die Zeile, die Sie ändern möchten.
   b. Kopieren Sie die kommentierte Zeile.
   c. Entkommentieren Sie den kopierten Text, indem Sie das Pfund (#)-Zeichen entfernen.
   d. Ändern Sie den Wert.
4. Speichern Sie die Datei, nachdem Sie Ihre Änderungen vorgenommen haben.

   SnapDrive für UNIX prüft diese Datei automatisch jedes Mal, wenn sie startet. Sie müssen den SnapDrive for UNIX Daemon neu starten, damit die Änderungen wirksam werden.