Konfigurieren und Anwenden von Audit-Richtlinien auf NTFS-Dateien und -Ordner mithilfe der CLI

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

Konfigurieren und Anwenden von Audit-Richtlinien auf NTFS-Dateien und -Ordner mithilfe der CLI-Übersicht

Sie müssen mehrere Schritte durchführen, um Überwachungsrichtlinien auf NTFS-Dateien und -Ordner anzuwenden, wenn Sie die ONTAP-CLI verwenden. Zunächst erstellen Sie einen NTFS-Sicherheitsdeskriptor und fügen SACLs zum Sicherheitsdeskriptor hinzu. Als nächstes erstellen Sie eine Sicherheitsrichtlinie und fügen Sie Richtlinienaufgaben hinzu. Anschließend wenden Sie die Sicherheitsrichtlinie auf eine Storage Virtual Machine (SVM) an.

Über diese Aufgabe

Nachdem Sie die Sicherheitsrichtlinie angewendet haben, können Sie den Job der Sicherheitsrichtlinie überwachen und anschließend die Einstellungen für die angewendete Überwachungsrichtlinie überprüfen.

> Wenn eine Audit-Richtlinie und die zugehörigen SACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Sie sollten vorhandene Sicherheitsrichtlinien überprüfen, bevor Sie neue erstellen und anwenden.

Verwandte Informationen

Dateizugriff wird mithilfe von Storage-Level Access Guard gesichert

Einschränkungen bei der Verwendung der CLI zum Festlegen der Datei- und Ordnersicherheit

Anwenden von Sicherheitsdeskriptoren zur Anwendung der Datei- und Ordnersicherheit

"SMB- und NFS-Auditing und Sicherheits-Tracing"

Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI

Erstellen Sie einen NTFS-Sicherheitsdeskriptor

Das Erstellen einer NTFS-Überwachungsrichtlinie für Sicherheitsdeskriptor ist der erste Schritt bei der Konfiguration und Anwendung von NTFS-Zugriffssteuerungslisten (NTFS Access Control Lists, ACLs) auf Dateien und Ordner in SVMs. Sie verknüpfen den Sicherheitsdeskriptor mit dem Datei- oder Ordnerpfad in einer Richtlinienaufgabe.

Über diese Aufgabe

NTFS-Sicherheitsdeskriptoren können für Dateien und Ordner erstellt werden, die sich in NTFS-Volumes im Sicherheitsstil befinden, oder für Dateien und Ordner, die sich auf gemischten Volumes im Sicherheitsstil befinden.

Wenn ein Sicherheitsdeskriptor erstellt wird, werden standardmäßig vier DACL-Einträge (Discretionary Access Control List) zur Sicherheitsbeschreibung hinzugefügt. Die vier Standard-Aces sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Anwenden der Berechtigungen
BUILTIN\Administratoren	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
BUILTIN\Benutzer	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
CREATOR-BESITZER	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Besitzer des Sicherheitsdeskriptors
- Primäre Gruppe des Eigentümers
- RAW-Kontrollfahnen

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Schritte

1. Wenn Sie die erweiterten Parameter verwenden möchten, setzen Sie die Berechtigungsebene auf erweitert: `set -privilege advanced`
2. Sicherheitsdeskriptor erstellen: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Vergewissern Sie sich, dass die Konfiguration des Sicherheitsdeskriptors korrekt ist: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                 Vserver: vs1
                   Security Descriptor Name: sd1
                Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Wenn Sie sich auf der erweiterten Berechtigungsebene befinden, kehren Sie zur Admin-Berechtigungsebene zurück: `set -privilege admin`

Fügen Sie NTFS SACL-Zugriffssteuerungseinträge zum NTFS-Sicherheitsdeskriptor hinzu

Das Hinzufügen von SACL (System Access Control List) Access Control Entries (Aces) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Erstellung von NTFS-Audit-Richtlinien für Dateien oder Ordner in SVMs. Jeder Eintrag identifiziert den Benutzer oder die Gruppe, die Sie prüfen möchten. Der SACL-Eintrag definiert, ob Sie erfolgreiche oder fehlgeschlagene Zugriffsversuche prüfen möchten.

Über diese Aufgabe

Sie können eine oder mehrere Asse zur SACL des Sicherheitsdeskriptors hinzufügen.

Wenn der Sicherheitsdeskriptor eine SACL enthält, die Asse enthält, fügt der Befehl den neuen ACE zur SACL hinzu. Wenn der Sicherheitsdeskriptor keine SACL enthält, erstellt der Befehl die SACL und fügt diesem den neuen ACE hinzu.

Sie können SACL-Einträge konfigurieren, indem Sie angeben, welche Rechte Sie für erfolgreiche Ereignisse oder Fehlerereignisse für das in angegebene Konto prüfen möchten `-account` Parameter. Es gibt drei Methoden, die sich gegenseitig ausschließen, um Rechte anzugeben:

- Rechte
- Erweiterte Rechte
- RAW-Rechte (Advanced-Privilege)

> Wenn Sie keine Rechte für den SACL-Eintrag angeben, ist die Standardeinstellung `Full Control`.

Sie können optional SACL-Einträge anpassen, indem Sie festlegen, wie Vererbung mit dem angewendet wird `apply to` Parameter. Wenn Sie diesen Parameter nicht angeben, wird dieser SACL-Eintrag standardmäßig auf diesen Ordner, Unterordner und Dateien angewendet.

Schritte

1. Hinzufügen eines SACL-Eintrags zu einem Sicherheitsdeskriptor: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Vergewissern Sie sich, dass die SACL-Eingabe korrekt ist: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                            Vserver: vs1
                  Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
                     Account Name or SID: DOMAIN\joe
                           Access Rights: full-control
                  Advanced Access Rights: -
                                Apply To: this-folder
                           Access Rights: full-control
```

Erstellen von Sicherheitsrichtlinien

Das Erstellen einer Audit-Richtlinie für Storage Virtual Machines (SVMs) ist der dritte Schritt bei der Konfiguration und Anwendung von ACLs auf eine Datei oder einen Ordner. Eine Richtlinie fungiert als Container für verschiedene Aufgaben, wobei jede Aufgabe ein einzelner Eintrag ist, der auf Dateien oder Ordner angewendet werden kann. Sie können Aufgaben später der Sicherheitsrichtlinie hinzufügen.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollten Sie die Sicherheitsrichtlinie jeder Storage Virtual Machine (SVM) zuordnen (mit NTFS-Volumes im Sicherheitsstil oder gemischten Volumes im Sicherheitsstil).

Schritte

1. Sicherheitsrichtlinie erstellen: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory policy create -policy-name policy1 -vserver vs1
   ```

2. Überprüfen Sie die Sicherheitsrichtlinie: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Fügen Sie der Sicherheitsrichtlinie eine Aufgabe hinzu

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt bei der Konfiguration und Anwendung von ACLs auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe verknüpfen Sie die Aufgabe mit einer Sicherheitsrichtlinie. Sie können einer Sicherheitsrichtlinie einen oder mehrere

Aufgabeneinträge hinzufügen.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf einen einzelnen Vorgang, der von einer Sicherheitsrichtlinie auf Dateien oder Ordner mit NTFS oder gemischter Sicherheit (oder auf ein Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. ACLs, die über Datei- und Verzeichnisaufgaben angewendet werden, können mit SMB-Clients oder der ONTAP CLI gemanagt werden.

- Storage-Level Access Guard-Aufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf Storage-Ebene für den Access Guard auf ein angegebenes Volume anwenden. ACLs, die über Aufgaben der Storage-Ebene Access Guard angewendet werden, können nur über die ONTAP-CLI gemanagt werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder eines Dateiansatz (oder Ordners). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Es kann nur eine Aufgabe pro Pfad innerhalb einer einzigen Richtlinie geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10,000 Aufgabeneinträge eingegeben werden.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Obwohl eine Richtlinie mehr als eine Aufgabe enthalten kann, können Sie eine Richtlinie nicht so konfigurieren, dass sie sowohl Dateiverzeichnisaufgaben als auch Zugriffsschutz auf Speicherebene enthält. Eine Richtlinie muss entweder alle Storage-Level Access Guard-Aufgaben oder alle Dateiverzeichnisaufgaben enthalten.

- Storage-Level Access Guard dient zur Einschränkung von Berechtigungen.

  Es wird niemals zusätzliche Zugriffsrechte geben.

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition
- Art der Zugriffskontrolle

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Schritte

1. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor hinzu: `vserver security file-directory policy task add -vserver vserver_name -policy -name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` Ist der Standardwert für `-access-control` Parameter. Die Angabe des Zugriffsteuerungstyps bei der Konfiguration von Aufgaben für den Datei- und Verzeichniszugriff ist optional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Überprüfen Sie die Aufgabenkonfiguration der Richtlinie: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Wenden Sie Sicherheitsrichtlinien an

Anwenden einer Audit-Richtlinie auf SVMsis der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie festgelegten Sicherheitseinstellungen auf NTFS-Dateien und Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder unterschiedlicher Sicherheitsstil).

Schritt

1. Anwenden einer Sicherheitsrichtlinie: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   Der Policy Apply Job ist geplant und die Job-ID wird zurückgegeben.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 –id
   53322" command to view the status of the operation
   ```

Überwachen Sie den Job der Sicherheitsrichtlinie

Wenn Sie die Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) anwenden, können Sie den Fortschritt der Aufgabe durch Monitoring des Jobs mit den Sicherheitsrichtlinien überwachen. Dies ist hilfreich, wenn Sie feststellen möchten, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn Sie einen langen Job haben, bei dem Sie Massensicherheit auf eine große Anzahl von Dateien und Ordnern anwenden.

Über diese Aufgabe

Um detaillierte Informationen über einen Job für Sicherheitsrichtlinien anzuzeigen, sollten Sie den verwenden `-instance` Parameter.

Schritt

1. Überwachen Sie den Job der Sicherheitsrichtlinie: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

Überprüfen Sie die angewandte Prüfungsrichtlinie

Sie können die Audit-Richtlinie überprüfen, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die Sie die Sicherheitsrichtlinie angewendet haben, die gewünschten Audit-Sicherheitseinstellungen aufweisen.

Über diese Aufgabe

Sie verwenden das `vserver security file-directory show` Befehl zum Anzeigen von Informationen zu Audit-Richtlinien. Sie müssen den Namen der SVM angeben, die die Daten und den Pfad zu den Daten enthält, deren Audit-Richtlinien für die Datei oder den Ordner angezeigt werden sollen.

Schritt

1. Einstellungen für Überwachungsrichtlinien anzeigen: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Beispiel

Mit dem folgenden Befehl werden die Informationen zur Audit-Richtlinie angezeigt, die auf den Pfad „`/corp`“ in SVM vs1 angewendet wurden. Der Pfad hat sowohl EINEN ERFOLG als auch einen ERFOLG/FEHLER SACL-Eintrag angewendet:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```