Verwalten Sie den Dateizugriff mit SMB

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/local-users-groups-concepts-concept.html on September 12, 2024. Always check docs.netapp.com for the latest.

Inhalt

Verwalten Sie den Dateizugriff mit SMB . . . 1
Verwenden Sie lokale Benutzer und Gruppen zur Authentifizierung und Autorisierung . . . 1
Konfigurieren Sie die Überprüfung der Bypass-Traverse . . . 28
Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an . . . 31
Managen Sie NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf SVMs über die CLI . . . 51
Konfigurieren Sie den Metadaten-Cache für SMB-Freigaben . . . 77
Verwalten von Dateisperren . . . 78
Überwachen Sie die SMB-Aktivitäten . . . 83

Verwalten Sie den Dateizugriff mit SMB

Verwenden Sie lokale Benutzer und Gruppen zur Authentifizierung und Autorisierung

Wie ONTAP lokale Benutzer und Gruppen verwendet

Lokale Benutzer und Gruppen Konzepte

Sie sollten wissen, was lokale Benutzer und Gruppen sind, und einige grundlegende Informationen über sie, bevor Sie bestimmen, ob lokale Benutzer und Gruppen in Ihrer Umgebung konfigurieren und verwenden.

- **Lokaler Benutzer**

  Ein Benutzerkonto mit einer eindeutigen Sicherheitskennung (SID), die nur für die Storage Virtual Machine (SVM) sichtbar ist, auf der sie erstellt wird. Lokale Benutzerkonten haben eine Reihe von Attributen, einschließlich Benutzername und SID. Ein lokales Benutzerkonto authentifiziert sich lokal auf dem CIFS-Server mithilfe der NTLM-Authentifizierung.

  Benutzerkonten verfügen über verschiedene Verwendungsmöglichkeiten:

  - Wird verwendet, um einem Benutzer „*User Rights Management* -Berechtigungen zu gewähren.
  - Kontrolliert den Zugriff auf Datei- und Ordnerressourcen, die der SVM zur Verfügung stehen.
- **Lokale Gruppe**

  Eine Gruppe mit einer eindeutigen SID hat nur Sichtbarkeit auf der SVM, auf der sie erstellt wird. Gruppen enthalten einen Satz Mitglieder. Mitglieder können lokale Benutzer, Domänenbenutzer, Domänengruppen und Domain-Machine-Konten sein. Gruppen können erstellt, geändert oder gelöscht werden.

  Gruppen haben verschiedene Verwendungszwecke:

  - Wird verwendet, um seinen Mitgliedern_User Rights Management_ Berechtigungen zu gewähren.
  - Kontrolliert den Zugriff auf Datei- und Ordnerressourcen, die der SVM zur Verfügung stehen.
- **Lokale Domain**

  Eine Domäne mit lokalem Umfang, der von der SVM begrenzt wird. Der Name der lokalen Domäne ist der CIFS-Servername. Lokale Benutzer und Gruppen sind in der lokalen Domäne enthalten.

- **Sicherheitskennung (SID)**

  Ein SID ist ein numerischer Wert mit variabler Länge, der Sicherheitsgrundel im Windows-Stil identifiziert. Ein typischer SID hat beispielsweise die folgende Form: S-1-5-21-3139654847-1303905135-2517279418-123456.

- * NTLM-Authentifizierung*

  Eine Microsoft Windows-Sicherheitsmethode zur Authentifizierung von Benutzern auf einem CIFS-Server.

- **Cluster replizierte Datenbank (RDB)**

Eine replizierte Datenbank mit einer Instanz an jedem Node in einem Cluster. Lokale Benutzer- und Gruppenobjekte werden in der RDB gespeichert.

Gründe für das Erstellen von lokalen Benutzern und lokalen Gruppen

Es gibt mehrere Gründe, warum Sie lokale Benutzer und lokale Gruppen auf Ihrer Storage Virtual Machine (SVM) erstellen sollten. Sie können beispielsweise über ein lokales Benutzerkonto auf einen SMB-Server zugreifen, wenn die Domänencontroller (DCs) nicht verfügbar sind, Sie lokale Gruppen zum Zuweisen von Berechtigungen verwenden möchten oder sich Ihr SMB-Server in einer Arbeitsgruppe befindet.

Aus folgenden Gründen können Sie ein oder mehrere lokale Benutzerkonten erstellen:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänenbenutzer sind nicht verfügbar.

  Lokale Benutzer sind in Arbeitsgruppen-Konfigurationen erforderlich.

- Sie möchten die Möglichkeit haben, sich beim SMB-Server zu authentifizieren und anzumelden, wenn die Domänencontroller nicht verfügbar sind.

  Lokale Benutzer können sich beim Ausfall des Domänencontrollers mit dem SMB-Server durch NTLM-Authentifizierung authentifizieren oder wenn Netzwerkprobleme verhindern, dass Ihr SMB-Server den Domänencontroller kontaktiert.

- Sie möchten einem lokalen Benutzer die Berechtigungen „*User Rights Management*“ zuweisen.

  User Rights Management bietet einem SMB-Serveradministrator die Möglichkeit, die Rechte der Benutzer und Gruppen auf der SVM zu kontrollieren. Sie können einem Benutzer Berechtigungen zuweisen, indem Sie dem Konto des Benutzers die Berechtigungen zuweisen oder den Benutzer zu einem Mitglied einer lokalen Gruppe mit diesen Berechtigungen machen.

Aus folgenden Gründen können Sie eine oder mehrere lokale Gruppen erstellen:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänengruppen sind nicht verfügbar.

  Lokale Gruppen sind in Arbeitsgruppen-Konfigurationen nicht erforderlich, können aber für die Verwaltung von Zugriffsberechtigungen für Benutzer lokaler Arbeitsgruppen nützlich sein.

- Sie möchten den Zugriff auf Datei- und Ordnerressourcen steuern, indem Sie lokale Gruppen zur Freigabe- und Dateizugriffskontrolle verwenden.
- Sie möchten lokale Gruppen mit benutzerdefinierten Berechtigungen *User Rights Management* erstellen.

  Einige integrierte Benutzergruppen haben vordefinierte Berechtigungen. Um einen benutzerdefinierten Satz von Berechtigungen zuzuweisen, können Sie eine lokale Gruppe erstellen und dieser Gruppe die erforderlichen Berechtigungen zuweisen. Anschließend können Sie der lokalen Gruppe lokale Benutzer, Domänenbenutzer und Domänengruppen hinzufügen.

Verwandte Informationen

Funktionsweise der lokalen Benutzerauthentifizierung

Liste der unterstützten Berechtigungen

Funktionsweise der lokalen Benutzerauthentifizierung

Bevor ein lokaler Benutzer auf Daten auf einem CIFS-Server zugreifen kann, muss er eine authentifizierte Sitzung erstellen.

Da SMB auf Sitzungen basiert ist, kann die Identität des Benutzers nur einmal bestimmt werden, wenn die Sitzung zum ersten Mal eingerichtet wird. Der CIFS-Server verwendet bei der Authentifizierung lokaler Benutzer eine NTLM-basierte Authentifizierung. Sowohl NTLMv1 als auch NTLMv2 werden unterstützt.

Bei ONTAP wird die lokale Authentifizierung in drei Anwendungsfällen eingesetzt. Jeder Anwendungsfall hängt davon ab, ob der Domain-Teil des Benutzernamens (mit DOMAIN\User Format) mit dem lokalen Domain-Namen des CIFS-Servers (der CIFS-Servername) übereinstimmt:

- Der Domain-Teil stimmt überein

  Benutzer, die lokale Benutzeranmeldeinformationen bereitstellen, wenn sie Zugriff auf Daten anfordern, werden lokal auf dem CIFS-Server authentifiziert.

- Der Domain-Teil stimmt nicht überein

  ONTAP versucht, NTLM-Authentifizierung mit einem Domain Controller in der Domäne zu verwenden, zu der der CIFS-Server gehört. Wenn die Authentifizierung erfolgreich ist, ist die Anmeldung abgeschlossen. Wenn es nicht gelingt, was als nächstes geschieht, hängt davon ab, warum die Authentifizierung nicht erfolgreich war.

  Wenn der Benutzer beispielsweise in Active Directory existiert, das Passwort jedoch ungültig oder abgelaufen ist, versucht ONTAP nicht, das entsprechende lokale Benutzerkonto auf dem CIFS-Server zu verwenden. Stattdessen schlägt die Authentifizierung fehl. In anderen Fällen verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server, sofern es existiert, für die Authentifizierung - auch wenn die NetBIOS-Domänennamen nicht übereinstimmen. Wenn beispielsweise ein passendes Domänenkonto existiert, es aber deaktiviert ist, verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server zur Authentifizierung.

- Der Domain-Teil wurde nicht angegeben

  ONTAP versucht zum ersten Mal, die Authentifizierung als lokaler Benutzer zu aktivieren. Wenn die Authentifizierung als lokaler Benutzer fehlschlägt, dann authentifiziert ONTAP den Benutzer mit einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört.

Nachdem die lokale Benutzerauthentifizierung oder die Domänenbenutzerauthentifizierung erfolgreich abgeschlossen wurde, baut ONTAP ein komplettes Benutzerzugriffstoken auf, das die Mitgliedschaft und Berechtigungen der lokalen Gruppe berücksichtigt.

Weitere Informationen zur NTLM-Authentifizierung für lokale Benutzer finden Sie in der Microsoft Windows-Dokumentation.

Verwandte Informationen

Aktivieren oder Deaktivieren der lokalen Benutzerauthentifizierung

Wie Benutzer-Access-Token erstellt werden

Wenn ein Benutzer eine Freigabe zuordnet, wird eine authentifizierte SMB-Sitzung eingerichtet und ein Benutzer-Access-Token erstellt, das Informationen über den Benutzer, die Gruppenmitgliedschaft des Benutzers und die kumulativen Berechtigungen

sowie den zugeordneten UNIX-Benutzer enthält.

Sofern die Funktion nicht deaktiviert ist, werden dem Benutzer- und Gruppeninformationen auch lokale Benutzer- und Gruppeninformationen hinzugefügt. Die Art und Weise, wie Access Tokens aufgebaut werden, hängt davon ab, ob sich die Anmeldung für einen lokalen Benutzer oder einen Active Directory-Domänenbenutzer befindet:

- Lokale Benutzeranmeldung

  Obwohl lokale Benutzer Mitglieder verschiedener lokaler Gruppen sein können, können lokale Gruppen nicht Mitglieder anderer lokaler Gruppen sein. Das lokale Benutzer-Zugriffstoken besteht aus einer Vereinigung aller Berechtigungen, die Gruppen zugewiesen sind, denen ein bestimmter lokaler Benutzer Mitglied ist.

- Anmeldung für Domänenbenutzer

  Wenn sich ein Domänenbenutzer anmeldet, erhält ONTAP ein Benutzerzugriffstoken, das die Benutzer-SID und SIDs für alle Domänengruppen enthält, zu denen der Benutzer Mitglied ist. ONTAP verwendet die Vereinigung des Zugriffstoken für Domänenbenutzer mit dem Zugriffstoken, das von lokalen Mitgliedschaften der Domänengruppen des Benutzers bereitgestellt wird (falls vorhanden), sowie allen direkten Berechtigungen, die dem Domänenbenutzer oder seiner Domänengruppmitgliedschaften zugewiesen sind.

Sowohl bei der lokalen Anmeldung als auch bei der Domain-Anmeldung wird die primäre GRUPPENLOSUNG auch für das Benutzerzugriffstoken festgelegt. Die Standard-RID ist `Domain Users` (513). Sie können den Standardwert nicht ändern.

Die Namenszuordnungen von Windows-zu-UNIX und UNIX-zu-Windows befolgen dieselben Regeln für lokale und Domänenkonten.

> Es gibt keine implizierte automatische Zuordnung von einem UNIX-Benutzer zu einem lokalen Konto. Ist dies erforderlich, muss mithilfe der vorhandenen Befehle für die Namenszuordnung eine explizite Zuordnungsregel angegeben werden.

Richtlinien zur Verwendung von SnapMirror auf SVMs, die lokale Gruppen enthalten

Beachten Sie die Richtlinien bei der Konfiguration von SnapMirror auf Volumes von SVMs, die lokale Gruppen enthalten.

Sie können keine lokalen Gruppen in Aces verwenden, die auf Dateien, Verzeichnisse oder Freigaben angewendet werden, die von SnapMirror auf eine andere SVM repliziert werden. Wenn Sie mithilfe der SnapMirror Funktion eine DR-Spiegelung für ein Volume auf einer anderen SVM erstellen und das Volume über einen ACE für eine lokale Gruppe verfügt, ist der ACE auf dem Spiegel nicht gültig. Wenn die Daten in eine andere SVM repliziert werden, werden sie effektiv in eine andere lokale Domäne überführt. Die Berechtigungen für lokale Benutzer und Gruppen gelten nur für den Umfang der SVM, auf der sie ursprünglich erstellt wurden.

Was passiert mit lokalen Benutzern und Gruppen beim Löschen von CIFS-Servern

Der Standardsatz lokaler Benutzer und Gruppen wird bei Erstellung eines CIFS-Servers erstellt und mit der Storage Virtual Machine (SVM) verknüpft, die den CIFS-Server hostet. SVM-Administratoren können jederzeit lokale Benutzer und Gruppen erstellen. Sie

müssen sich bewusst sein, was mit lokalen Benutzern und Gruppen passiert, wenn Sie den CIFS Server löschen.

Lokale Benutzer und Gruppen sind SVMs zugeordnet. Daher werden sie nicht gelöscht, wenn CIFS Server aus Sicherheitsgründen gelöscht werden. Lokale Benutzer und Gruppen werden zwar nicht gelöscht, wenn der CIFS-Server gelöscht wird, sind aber ausgeblendet. Sie können lokale Benutzer und Gruppen erst anzeigen oder managen, wenn Sie einen CIFS-Server auf der SVM neu erstellen.

> Der Administrationsstatus des CIFS-Servers hat keine Auswirkung auf die Sichtbarkeit lokaler Benutzer oder Gruppen.

Wie Sie Microsoft Management Console mit lokalen Benutzern und Gruppen verwenden können

Sie können Informationen zu lokalen Benutzern und Gruppen in der Microsoft Management Console anzeigen. Mit diesem Release von ONTAP können Sie keine anderen Verwaltungsaufgaben für lokale Benutzer und Gruppen über die Microsoft Verwaltungskonsole ausführen.

Richtlinien zum Zurücksetzen

Wenn Sie das Cluster auf eine ONTAP Version zurücksetzen möchten, die lokale Benutzer und Gruppen nicht unterstützt, und lokale Benutzer und Gruppen für das Management des Dateizugriffs oder von Benutzerrechten verwendet werden, müssen Sie sich über bestimmte Überlegungen im Klaren sein.

- Aus Sicherheitsgründen werden Informationen zu konfigurierten lokalen Benutzern, Gruppen und Berechtigungen nicht gelöscht, wenn ONTAP auf eine Version zurückgesetzt wird, die keine lokalen Benutzer- und Gruppenfunktionen unterstützt.
- Bei einem Zurücksetzen auf eine vorherige Hauptversion von ONTAP verwendet ONTAP während der Authentifizierung und der Erstellung von Anmeldeinformationen keine lokalen Benutzer und Gruppen.
- Lokale Benutzer und Gruppen werden nicht aus Datei- und Ordner-ACLs entfernt.
- Zugriffsanfragen, die vom Zugriff abhängig sind, die aufgrund von Berechtigungen für lokale Benutzer oder Gruppen gewährt werden, werden verweigert.

  Um den Zugriff zu ermöglichen, müssen Sie Dateiberechtigungen neu konfigurieren, um den Zugriff auf der Basis von Domänenobjekten anstelle von lokalen Benutzer- und Gruppenobjekten zu ermöglichen.

Welche lokalen Berechtigungen sind

Liste der unterstützten Berechtigungen

ONTAP verfügt über einen vordefinierten Satz unterstützter Berechtigungen. Bestimmte vordefinierte lokale Gruppen haben einige dieser Berechtigungen standardmäßig hinzugefügt. Sie können außerdem Berechtigungen aus den vordefinierten Gruppen hinzufügen oder entfernen oder neue lokale Benutzer oder Gruppen erstellen und den von Ihnen erstellten Gruppen oder vorhandenen Domänenbenutzern und -Gruppen Berechtigungen hinzufügen.

In der folgenden Tabelle werden die unterstützten Berechtigungen auf der Storage Virtual Machine (SVM) aufgeführt und eine Liste der BUILTIN-Gruppen mit zugewiesenen Berechtigungen angezeigt:

Berechtigungsname	Standardeinstellung für die Sicherheit	Beschreibung
`SeTcbPrivilege`	Keine	Als Teil des Betriebssystems agieren
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Sichern Sie Dateien und Verzeichnisse, und überschreiben Sie alle ACLs
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Wiederherstellung von Dateien und Verzeichnissen, Überschreiben aller ACLs setzt alle gültigen Benutzer- oder Gruppen-SID als Eigentümer der Datei
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Übernehmen Sie die Verantwortung für Dateien oder andere Objekte
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Verwaltung von Audits Dies umfasst das Anzeigen, Dumping und Löschen des Sicherheitsprotokolls.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Prüfung der Traverse umgehen Benutzer mit dieser Berechtigung benötigen keine Traverse (x)-Berechtigungen zum Traverse von Ordnern, Symlinks oder Kreuzungen.

Verwandte Informationen

- Weisen Sie lokale Berechtigungen zu
- Konfigurieren der Umgehungsüberprüfung

Berechtigungen zuweisen

Sie können lokalen Benutzern oder Domänenbenutzern Berechtigungen direkt zuweisen. Alternativ können Sie lokalen Gruppen Benutzer zuweisen, deren zugewiesene Berechtigungen den Fähigkeiten entsprechen, die diese Benutzer haben sollen.

- Sie können einer von Ihnen erstellten Gruppe einen Satz von Berechtigungen zuweisen.

  Anschließend fügen Sie der Gruppe einen Benutzer hinzu, der über die Berechtigungen verfügt, über die dieser Benutzer verfügen soll.

- Sie können auch lokale Benutzer und Domänenbenutzer vordefinierten Gruppen zuweisen, deren Standardberechtigungen mit den Berechtigungen übereinstimmen, die Sie diesen Benutzern gewähren möchten.

Verwandte Informationen

- Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -Gruppen
- Entfernen von Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen
- Zurücksetzen von Berechtigungen für lokale oder Domänenbenutzer und -Gruppen
- Konfigurieren der Umgehungsüberprüfung

Richtlinien für die Nutzung von BUILTIN-Gruppen und dem lokalen Administratorkonto

Es gibt bestimmte Richtlinien, die Sie beachten sollten, wenn Sie BUILTIN-Gruppen und das lokale Administratorkonto verwenden. Beispielsweise können Sie das lokale Administratorkonto umbenennen, dieses Konto kann jedoch nicht gelöscht werden.

- Das Administratorkonto kann umbenannt, aber nicht gelöscht werden.
- Das Administratorkonto kann nicht aus der BUILTIN\Administrators-Gruppe entfernt werden.
- BUILTIN-Gruppen können umbenannt, aber nicht gelöscht werden.

  Nachdem die BUILTIN-Gruppe umbenannt wurde, kann ein anderes lokales Objekt mit dem bekannten Namen erstellt werden; dem Objekt wird jedoch eine neue RID zugewiesen.

- Es gibt kein lokales Gastkonto.

Verwandte Informationen

Vordefinierte BUILTIN-Gruppen und Standardberechtigungen

Anforderungen für lokale Benutzerpasswörter

Standardmäßig müssen lokale Benutzerpasswörter den Komplexitätsanforderungen entsprechen. Die Anforderungen an die Passwortkomplexität ähneln den in der Microsoft Windows *Local Security Policy* definierten Anforderungen.

Das Passwort muss die folgenden Kriterien erfüllen:

- Muss mindestens sechs Zeichen lang sein
- Darf den Benutzernamen nicht enthalten
- Muss Zeichen aus mindestens drei der folgenden vier Kategorien enthalten:
  - Englische Großbuchstaben (A bis Z)
  - Englische Kleinbuchstaben (A bis z)
  - Basis 10 Ziffern (0 bis 9)
  - Sonderzeichen:

    ~ ! @ # % ^ & * _ - + = ` \ ( ) [ ] : ; ' < > , . ? /

Verwandte Informationen

Aktivieren oder Deaktivieren der erforderlichen Passwortkomplexität für lokale SMB-Benutzer

Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers

Ändern der Passwörter für lokales Benutzerkonto

Vordefinierte BUILTIN-Gruppen und Standardberechtigungen

Sie können einer vordefinierten Gruppe von BUILTIN-Gruppen, die von ONTAP bereitgestellt werden, die Mitgliedschaft eines lokalen Benutzers oder eines Domänenbenutzers zuweisen. Vordefinierte Gruppen verfügen über vordefinierte Berechtigungen.

In der folgenden Tabelle werden die vordefinierten Gruppen beschrieben:

Vordefinierte BUILTIN-Gruppe	Standardberechtigungen
`BUILTIN\Administrators`544 LOSWERDEN Beim ersten Erstellens wird der lokale erstellt `Administrator` Konto, mit einer RID von 500, wird automatisch ein Mitglied dieser Gruppe. Wenn die Storage Virtual Machine (SVM) zu einer Domäne hinzugefügt wird, wird das angezeigt `domain\Domain Admins` Die Gruppe wird der Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird der `domain\Domain Admins` Die Gruppe wird aus der Gruppe entfernt.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`547 LOSWERDEN Bei der ersten Erstellung verfügt diese Gruppe über keine Mitglieder. Mitglieder dieser Gruppe haben folgende Merkmale: • Es können lokale Benutzer und Gruppen erstellt und verwaltet werden. • Sie können sich selbst oder ein anderes Objekt dem nicht hinzufügen `BUILTIN\Administrators` Gruppieren.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`551 LOSWERDEN Bei der ersten Erstellung verfügt diese Gruppe über keine Mitglieder. Mitglieder dieser Gruppe können Lese- und Schreibberechtigungen für Dateien oder Ordner überschreiben, wenn sie mit Sicherungsziel geöffnet werden.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`

Vordefinierte BUILTIN-Gruppe	Standardberechtigungen
`BUILTIN\Users`545 LOSWERDEN Bei der ersten Erstellung hat diese Gruppe keine Mitglieder (außer dem impliziten `Authenticated Users` Sondergruppe). Wenn die SVM zu einer Domäne verbunden ist, wird der `domain\Domain Users` Die Gruppe wird dieser Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird der `domain\Domain Users` Die Gruppe wurde aus dieser Gruppe entfernt.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Diese Gruppe umfasst alle Benutzer, einschließlich Gäste (aber nicht anonyme Benutzer). Hierbei handelt es sich um eine implizite Gruppe mit einer impliziten Mitgliedschaft.	`SeChangeNotifyPrivilege`

Verwandte Informationen

Richtlinien für die Nutzung von BUILTIN-Gruppen und dem lokalen Administratorkonto

Liste der unterstützten Berechtigungen

Konfigurieren der Umgehungsüberprüfung

Aktivieren oder Deaktivieren der Funktionen für lokale Benutzer und Gruppen

Aktivieren oder Deaktivieren der Funktionsübersicht für lokale Benutzer und Gruppen

Bevor Sie lokale Benutzer und Gruppen für die Zugriffskontrolle von NTFS-Sicherheitsdaten verwenden können, müssen die Funktionen lokaler Benutzer und Gruppen aktiviert sein. Wenn Sie außerdem lokale Benutzer zur SMB-Authentifizierung verwenden möchten, muss die lokale Benutzerauthentifizierungsfunktion aktiviert sein.

Die Funktionen für lokale Benutzer und Gruppen und die lokale Benutzerauthentifizierung sind standardmäßig aktiviert. Wenn sie nicht aktiviert sind, müssen Sie sie aktivieren, bevor Sie lokale Benutzer und Gruppen konfigurieren und verwenden können. Sie können die Funktionen für lokale Benutzer und Gruppen jederzeit deaktivieren.

Zusätzlich zum ausdrücklichen Deaktivieren von Funktionen für lokale Benutzer und Gruppen deaktiviert ONTAP Funktionen für lokale Benutzer und Gruppen, wenn ein Node im Cluster auf eine ONTAP Version zurückgesetzt wird, die die Funktionen nicht unterstützt. Die Funktionen lokaler Benutzer und Gruppen sind erst aktiviert, wenn alle Nodes im Cluster eine Version von ONTAP ausführen, die sie unterstützt.

Verwandte Informationen

Lokale Benutzerkonten ändern

Ändern von lokalen Gruppen

Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu

Aktivieren oder Deaktivieren von lokalen Benutzern und Gruppen

Lokale Benutzer und Gruppen können für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktiviert oder deaktiviert werden. Die Funktion für lokale Benutzer und Gruppen ist standardmäßig aktiviert.

Über diese Aufgabe

Sie können lokale Benutzer und Gruppen beim Konfigurieren von SMB-Freigaben- und NTFS-Dateiberechtigungen verwenden und können optional lokale Benutzer zur Authentifizierung verwenden, wenn Sie eine SMB-Verbindung erstellen. Um lokale Benutzer für die Authentifizierung zu verwenden, müssen Sie außerdem die Authentifizierungsoption für lokale Benutzer und Gruppen aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass lokale Benutzer und Gruppen…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

3. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Das folgende Beispiel bietet lokale Benutzer und Gruppen-Funktionen auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

Aktivieren oder Deaktivieren der Authentifizierung für lokale Benutzer

Lokale Benutzerkonten aktivieren oder deaktivieren

Aktivieren oder Deaktivieren der Authentifizierung für lokale Benutzer

Die Authentifizierung von lokalen Benutzern für SMB-Zugriff auf Storage Virtual Machines (SVMs) lässt sich aktivieren oder deaktivieren. Die Standardeinstellung erlaubt die lokale Benutzerauthentifizierung. Dies ist nützlich, wenn die SVM keinen Domänencontroller kontaktieren kann oder Sie keine Zugriffssteuerungen auf Domänenebene verwenden möchten.

Bevor Sie beginnen

Lokale Benutzer und Gruppen müssen auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Sie können die lokale Benutzerauthentifizierung jederzeit aktivieren oder deaktivieren. Wenn Sie lokale Benutzer zur Authentifizierung beim Erstellen einer SMB-Verbindung verwenden möchten, müssen Sie auch die Option für lokale Benutzer und Gruppen des CIFS-Servers aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn die lokale Authentifizierung…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Das folgende Beispiel ermöglicht die lokale Benutzerauthentifizierung auf SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

Funktionsweise der lokalen Benutzerauthentifizierung

Aktivieren oder Deaktivieren von lokalen Benutzern und Gruppen

Lokale Benutzerkonten verwalten

Lokale Benutzerkonten ändern

Sie können ein lokales Benutzerkonto ändern, wenn Sie den vollständigen Namen oder die Beschreibung eines vorhandenen Benutzers ändern möchten und wenn Sie das Benutzerkonto aktivieren oder deaktivieren möchten. Sie können auch ein lokales Benutzerkonto umbenennen, wenn der Name des Benutzers kompromittiert ist oder eine Namensänderung für administrative Zwecke erforderlich ist.

Ihr Ziel ist	Geben Sie den Befehl ein…
Ändern Sie den vollständigen Namen des lokalen Benutzers	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` Wenn der vollständige Name ein Leerzeichen enthält, muss er in doppelte Anführungszeichen eingeschlossen werden.
Ändern Sie die Beschreibung des lokalen Benutzers	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` Wenn die Beschreibung ein Leerzeichen enthält, muss sie in doppelte Anführungszeichen eingeschlossen werden.
Aktivieren oder deaktivieren Sie das lokale Benutzerkonto	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is -account-disabled {true`
`false}`	Benennen Sie das lokale Benutzerkonto um

Beispiel

Im folgenden Beispiel wird der lokale Benutzer „`CIFS_SERVER\sue`“ als „`CIFS_SERVER\sue_New`“ auf der Storage Virtual Machine (SVM, früher Vserver genannt) vs1 umbenannt:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Lokale Benutzerkonten aktivieren oder deaktivieren

Sie aktivieren ein lokales Benutzerkonto, wenn der Benutzer über eine SMB-Verbindung auf Daten in der Storage Virtual Machine (SVM) zugreifen soll. Sie können auch ein

lokales Benutzerkonto deaktivieren, wenn dieser Benutzer nicht über SMB auf SVM-Daten zugreifen soll.

Über diese Aufgabe

Sie aktivieren einen lokalen Benutzer, indem Sie das Benutzerkonto ändern.

Schritt

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie das Benutzerkonto	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`
Deaktivieren des Benutzerkontos	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled true`

Ändern Sie die Passwörter für das lokale Benutzerkonto

Sie können das Kontokennwort eines lokalen Benutzers ändern. Dies kann nützlich sein, wenn das Kennwort des Benutzers kompromittiert wird oder wenn der Benutzer das Passwort vergessen hat.

Schritt

1. Ändern Sie das Passwort, indem Sie die entsprechende Aktion ausführen: `vserver cifs users-and-groups local-user set-password -vserver` *`vserver_name`* `-user-name` *`user_name`*

Beispiel

Im folgenden Beispiel wird das Passwort für den lokalen Benutzer „`CIFS_SERVER\sue`“ festgelegt, der mit der Storage Virtual Machine (SVM, früher unter dem Namen „Vserver“ bekannt) vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Verwandte Informationen

Aktivieren oder Deaktivieren der erforderlichen Passwortkomplexität für lokale SMB-Benutzer

Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers

Informationen zu lokalen Benutzern anzeigen

Sie können eine Liste aller lokalen Benutzer in einem Übersichtsformular anzeigen. Wenn Sie festlegen möchten, welche Kontoeinstellungen für einen bestimmten Benutzer konfiguriert sind, können Sie detaillierte Kontoinformationen für diesen Benutzer sowie die Kontoinformationen für mehrere Benutzer anzeigen. Mithilfe dieser Informationen können Sie feststellen, ob Sie die Einstellungen eines Benutzers ändern müssen, und auch Probleme mit der Authentifizierung oder dem Dateizugriff beheben.

Über diese Aufgabe

Es werden nie Informationen zum Passwort eines Benutzers angezeigt.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Informationen über alle Benutzer auf der Storage Virtual Machine (SVM) anzeigen	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
Anzeigen detaillierter Kontoinformationen für einen Benutzer	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

   Es gibt weitere optionale Parameter, die Sie wählen können, wenn Sie den Befehl ausführen. Weitere Informationen finden Sie auf der man-Seite.

Beispiel

Das folgende Beispiel zeigt Informationen über alle lokalen Benutzer auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- --------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Informationen zu Gruppenmitgliedschaften für lokale Benutzer anzeigen

Sie können Informationen darüber anzeigen, zu welchen lokalen Gruppen ein lokaler Benutzer gehört. Anhand dieser Informationen können Sie bestimmen, auf welchen Zugriff der Benutzer auf Dateien und Ordner zugreifen soll. Diese Informationen können nützlich sein, um zu bestimmen, welche Zugriffsrechte der Benutzer für Dateien und Ordner haben sollte, oder wenn Sie Probleme mit dem Dateizugriff beheben.

Über diese Aufgabe

Sie können den Befehl so anpassen, dass nur die Informationen angezeigt werden, die angezeigt werden sollen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Zeigt Informationen zur lokalen Benutzermitgliedschaft für einen bestimmten lokalen Benutzer an	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
Zeigen Sie lokale Benutzermitgliedungsinformationen für die lokale Gruppe an, von der dieser lokale Benutzer Mitglied ist	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Anzeigen von Informationen zur Benutzermitgliedschaft für lokale Benutzer, die einer bestimmten SVM (Storage Virtual Machine) zugeordnet sind	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Anzeige detaillierter Informationen für alle lokalen Benutzer auf einer angegebenen SVM	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden die Mitgliedsinformationen für alle lokalen Benutzer auf SVM vs1 angezeigt; Benutzer „`CIFS_SERVER\Administrator`“ ist Mitglied der Gruppe „`BUILTIN\Administrators`“ und „`CIFS_SERVER\sue`“ ist Mitglied der Gruppe „`CIFS_SERVER\g1`“:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Lokale Benutzerkonten löschen

Sie können lokale Benutzerkonten von Ihrer Storage Virtual Machine (SVM) löschen, wenn diese nicht mehr für die lokale SMB-Authentifizierung am CIFS-Server oder zur Bestimmung der Zugriffsrechte auf den Daten auf Ihrer SVM benötigt werden.

Über diese Aufgabe

Beachten Sie beim Löschen lokaler Benutzer Folgendes:

- Das Dateisystem wird nicht verändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die auf diesen Benutzer verweisen, werden nicht angepasst.

- Alle Verweise auf lokale Benutzer werden aus den Mitgliedschafts- und Berechtigungsdatenbanken entfernt.
- Bekannte Standardbenutzer wie Administrator können nicht gelöscht werden.

Schritte

1. Legen Sie den Namen des lokalen Benutzerkontos fest, das Sie löschen möchten: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. Lokalen Benutzer löschen: `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. Vergewissern Sie sich, dass das Benutzerkonto gelöscht wurde: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel wird der lokale Benutzer „`CIFS_SERVER\sue`“ gelöscht, der mit SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Verwaltung lokaler Gruppen

Ändern von lokalen Gruppen

Sie können vorhandene lokale Gruppen ändern, indem Sie die Beschreibung für eine vorhandene lokale Gruppe ändern oder die Gruppe umbenennen.

Ihr Ziel ist	Verwenden Sie den Befehl…
Ändern Sie die Beschreibung der lokalen Gruppe	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` Wenn die Beschreibung ein Leerzeichen enthält, muss sie in doppelte Anführungszeichen eingeschlossen werden.
Benennen Sie die lokale Gruppe um	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

Beispiele

Im folgenden Beispiel wird die lokale Gruppe „`CIFS_SERVER\Engineering`“ in „`CIFS_SERVER\Engineering_New`“ umbenannt:

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

Im folgenden Beispiel wird die Beschreibung der lokalen Gruppe „`CIFS_SERVER\Engineering`“ geändert:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Zeigt Informationen zu lokalen Gruppen an

Sie können eine Liste aller auf dem Cluster konfigurierten lokalen Gruppen oder auf einer angegebenen SVM (Storage Virtual Machine) anzeigen. Diese Informationen können nützlich sein, wenn Sie Probleme beim Dateizugriff bei den Daten in der SVM oder Problemen mit den Benutzerrechten (Berechtigungen) auf der SVM beheben.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über…	Geben Sie den Befehl ein…
Alle lokalen Gruppen im Cluster	`vserver cifs users-and-groups local-group show`
Alle lokalen Gruppen auf der SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

Es gibt weitere optionale Parameter, die Sie bei der Ausführung dieses Befehls auswählen können. Weitere Informationen finden Sie auf der man-Seite.

Beispiel

Das folgende Beispiel zeigt Informationen zu allen lokalen Gruppen auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Verwaltung der lokalen Gruppenmitgliedschaft

Sie können die lokale Gruppenmitgliedschaft verwalten, indem Sie lokale Benutzer oder Domänenbenutzer hinzufügen und entfernen oder Domänengruppen hinzufügen und entfernen. Dies ist nützlich, wenn Sie den Zugriff auf Daten anhand von Zugriffskontrollen, die in der Gruppe platziert sind, steuern möchten oder wenn Benutzer über Berechtigungen verfügen möchten, die dieser Gruppe zugeordnet sind.

Über diese Aufgabe

Richtlinien zum Hinzufügen von Mitgliedern zu einer lokalen Gruppe:

- Sie können keine Benutzer zur speziellen *everyone*-Gruppe hinzufügen.
- Die lokale Gruppe muss vorhanden sein, bevor Sie einen Benutzer hinzufügen können.
- Der Benutzer muss vorhanden sein, bevor Sie den Benutzer einer lokalen Gruppe hinzufügen können.
- Sie können einer anderen lokalen Gruppe keine lokale Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Gruppe zu einer lokalen Gruppe hinzuzufügen, muss Data ONTAP in der Lage sein, den Namen zu einem SID aufzulösen.

Richtlinien zum Entfernen von Mitgliedern aus einer lokalen Gruppe:

- Sie können keine Mitglieder aus der speziellen *everyone*-Gruppe entfernen.
- Die Gruppe, aus der Sie ein Mitglied entfernen möchten, muss vorhanden sein.
- ONTAP muss in der Lage sein, die Namen der Mitglieder zu lösen, die Sie aus der Gruppe zu einem entsprechenden SID entfernen möchten.

Schritt

1. Fügen Sie ein Mitglied einer Gruppe hinzu oder entfernen Sie es.

Ihr Ziel ist	Verwenden Sie dann den Befehl…
Ein Mitglied zu einer Gruppe hinzufügen	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Sie können eine kommagetrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die der angegebenen lokalen Gruppe hinzugefügt werden sollen.
Entfernen Sie ein Mitglied aus einer Gruppe	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Sie können eine durch Komma getrennte Liste der lokalen Benutzer, Domänenbenutzer oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden sollen.

Im folgenden Beispiel wird der lokalen Gruppe „`SMB_SERVER\sue`“ und der lokalen Gruppe „`AD_DOM\dom_eng`“ auf SVM vs1 ein lokaler Benutzer „`SMB_SERVER\Engineering`“ hinzugefügt:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

Im folgenden Beispiel werden die lokalen Benutzer „`SMB_SERVER\sue`“ und „`SMB_SERVER\james`“ aus der lokalen Gruppe „`SMB_SERVER\Engineering`“ auf SVM vs1 entfernt:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verwandte Informationen

Anzeigen von Informationen zu Mitgliedern von lokalen Gruppen

Zeigt Informationen zu Mitgliedern lokaler Gruppen an

Sie können eine Liste aller Mitglieder der lokalen Gruppen anzeigen, die auf dem Cluster oder auf einer angegebenen Storage Virtual Machine (SVM) konfiguriert sind. Diese Informationen können hilfreich sein, wenn Probleme mit dem Zugriff auf Dateien oder Probleme mit Benutzerrechten (Berechtigungen) behoben werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Mitglieder aller lokalen Gruppen auf dem Cluster	`vserver cifs users-and-groups local-group show-members`
Mitglieder aller lokalen Gruppen auf der SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden Informationen über Mitglieder aller lokalen Gruppen auf SVM vs1 angezeigt:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Lokale Gruppe löschen

Sie können eine lokale Gruppe von der Storage Virtual Machine (SVM) löschen, wenn sie nicht mehr zum ermitteln der Zugriffsrechte für Daten benötigt wird, die dieser SVM zugeordnet sind, oder wenn sie nicht mehr zum Zuweisen von SVM-Benutzerrechten (Berechtigungen) zu Gruppenmitgliedern benötigt wird.

Über diese Aufgabe

Beachten Sie beim Löschen von lokalen Gruppen Folgendes:

- Das Dateisystem wird nicht verändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die sich auf diese Gruppe beziehen, werden nicht angepasst.

- Wenn die Gruppe nicht vorhanden ist, wird ein Fehler zurückgegeben.
- Die spezielle *Everyone*-Gruppe kann nicht gelöscht werden.
- Integrierte Gruppen wie *BUILTIN\Administrators BUILTIN\Users* können nicht gelöscht werden.

Schritte

1. Geben Sie den Namen der lokalen Gruppe an, die Sie löschen möchten, indem Sie die Liste der lokalen Gruppen auf der SVM anzeigen: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Lokale Gruppe löschen: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Vergewissern Sie sich, dass die Gruppe gelöscht wurde: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel wird die lokale Gruppe „`CIFS_SERVER\Sales`“ gelöscht, die mit SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
```

Domänenbenutzer- und Gruppennamen in lokalen Datenbanken aktualisieren

Sie können den lokalen Gruppen eines CIFS-Servers Domänenbenutzer und -Gruppen hinzufügen. Diese Domänenobjekte sind in lokalen Datenbanken auf dem Cluster registriert. Wenn ein Domänenobjekt umbenannt wird, müssen die lokalen Datenbanken manuell aktualisiert werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) angeben, auf der Sie Domänennamen aktualisieren möchten.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie die entsprechende Aktion aus:

Wenn Sie Domänenbenutzer und -Gruppen aktualisieren möchten und…	Befehl
Domänenbenutzer und -Gruppen anzeigen, die erfolgreich aktualisiert wurden und die nicht aktualisiert werden konnten	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*
Zeigen Sie Domänenbenutzer und -Gruppen an, die erfolgreich aktualisiert wurden	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only false`
Nur die Domänenbenutzer und -Gruppen anzeigen, die nicht aktualisiert werden können	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only true`
Alle Statusinformationen zu Aktualisierungen unterdrücken	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-suppress -all-output true`

3. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Im folgenden Beispiel werden die Namen der Domänenbenutzer und Gruppen aktualisiert, die mit der Storage Virtual Machine (SVM, ehemals Vserver genannt) vs1 verknüpft sind. Für das letzte Update gibt es eine abhängige Kette von Namen, die aktualisiert werden müssen:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Lokale Berechtigungen verwalten

Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu

Sie können Benutzerrechte für lokale oder Domänenbenutzer oder -Gruppen verwalten, indem Sie Berechtigungen hinzufügen. Die hinzugefügten Berechtigungen überschreiben die Standardberechtigungen, die einem dieser Objekte zugewiesen sind. Dadurch erhalten Sie verbesserte Sicherheit, indem Sie die Berechtigungen eines Benutzers oder einer Gruppe anpassen können.

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, zu der Berechtigungen hinzugefügt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Beim Hinzufügen einer Berechtigung zu einem Objekt werden die Standardberechtigungen für diesen Benutzer oder diese Gruppe überschrieben. Beim Hinzufügen einer Berechtigung werden zuvor hinzugefügte Berechtigungen nicht entfernt.

Beim Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -Gruppen müssen Sie Folgendes beachten:

- Sie können eine oder mehrere Berechtigungen hinzufügen.
- Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Gruppe kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem er sich an den Domänencontroller wenden kann.

  Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Fügen Sie einem lokalen Benutzer oder einer Domänengruppe eine oder mehrere Berechtigungen hinzu: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Vergewissern Sie sich, dass die gewünschten Berechtigungen auf das Objekt angewendet werden: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Im folgenden Beispiel werden die Berechtigungen „`SeTcbPrivilege`“ und „`SeTakeownershipPrivilege`“ für den Benutzer „`CIFS_SERVER\sue`“ auf Storage Virtual Machine (SVM, ehemals Vserver) vs1 hinzugefügt:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Entfernen Sie Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen

Sie können Benutzerrechte für lokale oder Domänenbenutzer oder -Gruppen verwalten, indem Sie Berechtigungen entfernen. Dadurch erhalten Sie verbesserte Sicherheit, indem Sie die maximalen Berechtigungen von Benutzern und Gruppen anpassen können.

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, aus der Berechtigungen entfernt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Beim Entfernen von Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen müssen Sie Folgendes beachten:

- Sie können eine oder mehrere Berechtigungen entfernen.
- Wenn Sie Berechtigungen von einem Domänenbenutzer oder einer Gruppe entfernen, kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem Sie sich an den Domänencontroller wenden.

  Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Entfernen Sie mindestens eine Berechtigung von einem lokalen Benutzer oder einer Domänengruppe: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Überprüfen Sie, ob die gewünschten Berechtigungen aus dem Objekt entfernt wurden: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Im folgenden Beispiel werden die Berechtigungen „`SeTcbPrivilege`“ und „`SeTakeownershipPrivilege`“ des Benutzers „`CIFS_SERVER\sue`“ auf Storage Virtual Machine (SVM, ehemals Vserver) vs1 entfernt:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

Berechtigungen für lokale oder Domänenbenutzer und -Gruppen zurücksetzen

Sie können Berechtigungen für lokale Benutzer oder Domänenbenutzer und -Gruppen zurücksetzen. Dies kann nützlich sein, wenn Sie Änderungen an Berechtigungen für einen lokalen Benutzer oder eine Domänengruppe vorgenommen haben und diese Änderungen nicht mehr gewünscht oder erforderlich sind.

Über diese Aufgabe

Beim Zurücksetzen der Berechtigungen für einen lokalen oder Domänenbenutzer oder eine Gruppe werden alle Berechtigungseinträge für dieses Objekt entfernt.

Schritte

1. Zurücksetzen der Berechtigungen für einen lokalen Benutzer oder eine Domänenbenutzer oder -Gruppe: `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*
2. Vergewissern Sie sich, dass die Berechtigungen auf dem Objekt zurückgesetzt wurden: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiele

Im folgenden Beispiel werden die Berechtigungen des Benutzers „`CIFS_SERVER\sue`“ auf der Storage Virtual Machine (SVM, früher als Vserver bezeichnet) vs1 zurückgesetzt. Standardmäßig verfügen normale Benutzer über keine Berechtigungen, die mit ihren Konten verknüpft sind:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Das folgende Beispiel setzt die Berechtigungen für die Gruppe „`BUILTIN\Administrators`“ zurück und entfernt damit effektiv den Eintrag für Berechtigungen:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Zeigt Informationen zu Berechtigungsüberschreibungen an

Sie können Informationen über benutzerdefinierte Berechtigungen anzeigen, die Domänenkonten oder lokalen Benutzerkonten oder Gruppen zugewiesen sind. Anhand dieser Informationen können Sie feststellen, ob die gewünschten Benutzerrechte angewendet werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Diesen Befehl eingeben…
Benutzerdefinierte Berechtigungen für alle Domänen- und lokalen Benutzer und Gruppen auf der Storage Virtual Machine (SVM)	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
Benutzerdefinierte Berechtigungen für eine bestimmte Domäne oder einen lokalen Benutzer und eine bestimmte Gruppe auf der SVM	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

   Es gibt weitere optionale Parameter, die Sie bei der Ausführung dieses Befehls auswählen können. Weitere Informationen finden Sie auf der man-Seite.

Beispiel

Mit dem folgenden Befehl werden alle Berechtigungen angezeigt, die explizit lokalen oder Domänenbenutzern und Gruppen für SVM vs1 zugeordnet sind:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
--------- ---------------------   ---------------
vs1       BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                  SeRestorePrivilege
vs1       CIFS_SERVER\sue         SeTcbPrivilege
                                  SeTakeOwnershipPrivilege
```

Konfigurieren Sie die Überprüfung der Bypass-Traverse

Konfigurieren Sie die Übersicht zur Überprüfung der Bypass-Traverse

Bypass Traverse Checking ist ein Benutzerrecht (auch bekannt als *Privilege*), das bestimmt, ob ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen kann, auch wenn der Benutzer keine Berechtigungen auf dem durchlaufenen Verzeichnis hat. Sie sollten wissen, was passiert, wenn Umgehungsüberprüfung zuzulassen oder nicht zulässt und wie eine Umgehungsüberprüfung für Benutzer auf Storage Virtual Machines (SVMs) konfiguriert wird.

Was passiert, wenn die Überprüfung der Bypass-Traverse erlaubt oder nicht erlaubt wird

- Wenn ein Benutzer versucht, auf eine Datei zuzugreifen, überprüft ONTAP nicht die Traverse-Berechtigung für die Zwischenverzeichnisse, wenn er bestimmt, ob er Zugriff auf die Datei gewährt oder verweigert.
- Wenn nicht zulässig, überprüft ONTAP die Berechtigung zum Traverse (Ausführen) für alle Verzeichnisse im Pfad zur Datei.

  Wenn eines der Zwischenverzeichnisse nicht über „`X`“ (Traverse-Berechtigung) verfügt, verweigert ONTAP den Zugriff auf die Datei.

Konfigurieren Sie die Überprüfung der Bypass-Traverse

Sie können die Bypass-Traverse-Überprüfung mithilfe der ONTAP-CLI oder durch Konfiguration der Active Directory-Gruppenrichtlinien mit diesem Benutzerrecht konfigurieren.

Der `SeChangeNotifyPrivilege` Die Berechtigungskontrollen, ob Benutzer die Traverse-Kontrolle umgehen dürfen.

- Wenn Sie sie lokalen SMB-Benutzern oder -Gruppen in der SVM oder zu Domänenbenutzern oder -Gruppen hinzufügen, ist eine Überbrückung der Überbrückung möglich.
- Wenn Sie sie von lokalen SMB-Benutzern oder -Gruppen auf der SVM oder von Domain-Benutzern oder -Gruppen entfernen, ist die Bypass-Traverse-Überprüfung nicht möglich.

Standardmäßig haben die folgenden BUILTIN-Gruppen auf der SVM das Recht, die Traverse-Kontrolle zu umgehen:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`

- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Wenn Sie den Mitgliedern einer dieser Gruppen nicht erlauben möchten, die Traverse-Kontrolle zu umgehen, müssen Sie diese Berechtigung aus der Gruppe entfernen.

Bei der Konfiguration der Bypass-Traverse-Überprüfung für lokale SMB-Benutzer und -Gruppen auf der SVM müssen Sie Folgendes beachten:

- Wenn Sie Mitgliedern einer benutzerdefinierten lokalen oder Domänengruppe erlauben möchten, die Traverse-Prüfung zu umgehen, müssen Sie die hinzufügen `SeChangeNotifyPrivilege` Berechtigung für diese Gruppe.
- Wenn Sie einem einzelnen lokalen Benutzer oder Domänenbenutzer erlauben möchten, die Traverse-Prüfung zu umgehen und dieser Benutzer kein Mitglied einer Gruppe mit dieser Berechtigung ist, können Sie das hinzufügen `SeChangeNotifyPrivilege` Berechtigung für dieses Benutzerkonto.
- Sie können die Bypass-Traverse-Suche nach lokalen oder Domänenbenutzern oder -Gruppen deaktivieren, indem Sie das entfernen `SeChangeNotifyPrivilege` Berechtigung jederzeit.

> Um die Bypass-Travers-Suche nach bestimmten lokalen oder Domänenbenutzern oder -Gruppen zu deaktivieren, müssen Sie auch das entfernen `SeChangeNotifyPrivilege` Berechtigung von `Everyone` Gruppieren.

Verwandte Informationen

Benutzern oder Gruppen erlauben, die Überprüfung der Verzeichnisdurchgang zu umgehen

Benutzer oder Gruppen davon ablassen, die Überprüfung der Verzeichnisdurchgang zu umgehen

Konfigurieren Sie die Zeichenzuordnung für die Übersetzung von SMB-Dateinamen auf Volumes

Erstellen Sie SMB-Zugriffssteuerungslisten

Sicherer Dateizugriff über Storage-Level Access Guard

Liste der unterstützten Berechtigungen

Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu

Benutzern oder Gruppen erlauben, die Überprüfung der Verzeichnisdurchgang zu umgehen

Wenn Sie möchten, dass ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen kann, selbst wenn der Benutzer keine Berechtigungen in einem durchlaufenen Verzeichnis besitzt, können Sie das hinzufügen `SeChangeNotifyPrivilege` Berechtigung für lokale SMB-Benutzer oder Gruppen auf Storage Virtual Machines (SVMs). Standardmäßig können Benutzer die Verzeichnisprüfung umgehen.

Bevor Sie beginnen

- Auf der SVM muss ein SMB-Server vorhanden sein.
- Die Option für lokale Benutzer und SMB-Gruppen-Server muss aktiviert sein.
- Der lokale oder Domain-Benutzer oder die Gruppe, der der zugeordnet ist `SeChangeNotifyPrivilege` Berechtigungen müssen bereits vorhanden sein.

Über diese Aufgabe

Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Gruppe kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem er sich an den Domänencontroller wenden kann. Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Aktivieren Sie die Bypass-Traverse-Überprüfung, indem Sie das hinzufügen `SeChangeNotifyPrivilege` Berechtigung für einen lokalen oder Domänenbenutzer oder eine Gruppe: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   Der Wert für das `-user-or-group-name` Parameter ist ein lokaler Benutzer oder eine lokale Gruppe oder ein Domänenbenutzer oder -Gruppe.

2. Vergewissern Sie sich, dass für den angegebenen Benutzer oder die angegebene Gruppe die Bypass-Traverse-Überprüfung aktiviert ist: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Mit dem folgenden Befehl können Benutzer, die zur Gruppe „`EXAMPLE\eng`“ gehören, die Überprüfung der Verzeichnisdurchgang umgehen, indem sie das hinzufügen `SeChangeNotifyPrivilege` Berechtigung für die Gruppe:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

Verwandte Informationen

Benutzer oder Gruppen davon ablassen, die Überprüfung der Verzeichnisdurchgang zu umgehen

Benutzer oder Gruppen davon ablassen, die Überprüfung der Verzeichnisdurchgang zu umgehen

Wenn ein Benutzer nicht alle Verzeichnisse im Pfad zu einer Datei durchlaufen soll, weil der Benutzer keine Berechtigungen im durchlaufenen Verzeichnis hat, können Sie das entfernen `SeChangeNotifyPrivilege` Berechtigungen von lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs).

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, aus der Berechtigungen entfernt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Wenn Sie Berechtigungen von einem Domänenbenutzer oder einer Gruppe entfernen, kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem Sie sich an den Domänencontroller wenden. Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Bypass-Traversen-Überprüfung nicht zulassen: `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   Mit dem Befehl wird das entfernt `SeChangeNotifyPrivilege` Berechtigung vom lokalen Benutzer oder der Domänengruppe, die Sie mit dem Wert für das angeben `-user-or-group-name name` Parameter.

2. Vergewissern Sie sich, dass für den angegebenen Benutzer oder die angegebene Gruppe die Umgehungsüberprüfung deaktiviert ist: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Beispiel

Mit dem folgenden Befehl werden Benutzer, die zur Gruppe „`EXAMPLE\eng`“ gehören, nicht mehr bei der Überprüfung der Verzeichnisübergang unterstützt:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -----------------------
vs1       EXAMPLE\eng           -
```

Verwandte Informationen

Benutzern oder Gruppen erlauben, die Überprüfung der Verzeichnisdurchgang zu umgehen

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

Sie können Informationen zur Dateisicherheit auf Dateien und Verzeichnissen in Volumes

auf Storage Virtual Machines (SVMs) anzeigen. Sie können Informationen zu Audit-Richtlinien in FlexVol Volumes anzeigen. Wenn konfiguriert, können Sie Informationen über die Sicherheitseinstellungen der Speicherebene und der dynamischen Zugriffskontrolle auf FlexVol Volumes anzeigen.

Anzeigen von Informationen zur Dateisicherheit

Sie können Informationen zur Dateisicherheit auf Daten anzeigen, die in Volumes und qtrees (für FlexVol Volumes) enthalten sind. Hierzu zählen folgende Sicherheitsstile:

- NTFS
- UNIX
- Gemischt

Anzeigen von Informationen zu Audit-Richtlinien

Sie können Informationen zu Audit-Richtlinien für das Auditing von Zugriffsereignissen auf FlexVol Volumes über die folgenden NAS-Protokolle anzeigen:

- SMB (alle Versionen)
- NFSv4.x

Anzeigen von Informationen zur Sicherheit des Storage-Level Access Guard (SCHLACKE)

Die Sicherheit des Zugriffschutzes auf Storage-Ebene kann auf FlexVol Volumes und qtree Objekte mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt
- UNIX (wenn ein CIFS-Server auf der SVM konfiguriert ist, die das Volume enthält)

Anzeigen von Informationen zur DAC-Sicherheit (Dynamic Access Control

Die Sicherheit der dynamischen Zugriffssteuerung lässt sich auf ein Objekt innerhalb eines FlexVol-Volumes anwenden:

- NTFS
- Gemischt (wenn das Objekt NTFS-effektive Sicherheit hat)

Verwandte Informationen

Dateizugriff wird mithilfe von Storage-Level Access Guard gesichert

Anzeigen von Informationen zum Speicher-Level Access Guard

Zeigt Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes an

Sie können Informationen über die Datei- und Verzeichnissicherheit auf NTFS-Volumes im Sicherheitsstil anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen über DOS-Attribute. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu

überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Da NTFS Security-Style Volumes und qtrees bei der Ermittlung von Dateizugriffsrechten nur NTFS-Dateiberechtigungen und Windows-Benutzer sowie -Gruppen verwenden, enthalten UNIX-bezogene Ausgabefelder nur Informationen zu Bildschirmberechtigungen für UNIX-Dateien.
- Die ACL-Ausgabe wird für Dateien und Ordner mit NTFS-Sicherheit angezeigt.
- Da die Sicherheit des Storage-Level Access Guard im Root-Verzeichnis oder qtree konfiguriert werden kann, wird die Ausgabe für einen Volume- oder qtree-Pfad, wo der Storage-Level Access Guard konfiguriert ist, möglicherweise sowohl normale Datei-ACLs als auch Storage-Level Access Guard ACLs angezeigt.
- Die Ausgabe zeigt auch Informationen zu dynamischen Zugriffssteuerungsassen an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit mehr Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/vol4` In SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                 Vserver: vs1
                               File Path: /vol4
                       File Inode Number: 64
                          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:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Im folgenden Beispiel werden die Sicherheitsinformationen mit erweiterten Masken zum Pfad angezeigt `/data/engineering` In SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
```

```
            Unix User Id: 0
           Unix Group Id: 0
          Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...1 .... .... .... .... .... =
Synchronize
                             .... .... .... 1... .... .... .... .... =
Write Owner
                             .... .... .... .1.. .... .... .... .... =
Write DAC
                             .... .... .... ..1. .... .... .... .... =
Read Control
                             .... .... .... ...1 .... .... .... .... =
Delete
```

```
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
```

```
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

Im folgenden Beispiel werden Sicherheitsinformationen für das Volume mit dem Pfad angezeigt, einschließlich Sicherheitsinformationen auf Storage-Ebene Access Guard `/datavol1` In SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         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:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Verwandte Informationen

Anzeigen von Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart

Anzeigen von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Zeigt Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart an

Sie können Informationen über die Datei- und Verzeichnissicherheit auf Volumes mit gemischter Sicherheitsart anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu UNIX-Eigentümern und -Gruppen. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Ordner enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.
- Die oberste Ebene eines gemischten Volumes im Sicherheitsstil kann entweder UNIX oder NTFS effektiven Schutz haben.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Verzeichnisse, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).
- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, kann möglicherweise sowohl UNIX Dateiberechtigungen als auch Storage-Level Access Guard ACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS-effektiver Sicherheit besteht, zeigt die Ausgabe auch Informationen über Dynamic Access Control Aces an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/projects` In SVM vs1

als erweiterte Maske. Dieser Pfad im gemischten Sicherheitsstil verfügt über effektive UNIX-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/data` In SVM vs1. Dieser Pfad mit gemischtem Sicherheitsstil verfügt über eine NTFS-effektive Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                 Vserver: vs1
                               File Path: /data
                       File Inode Number: 544
                          Security Style: mixed
                         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:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Im folgenden Beispiel werden die Sicherheitsinformationen zum Volume im Pfad angezeigt `/datavol5` In SVM vs1. Auf der obersten Ebene dieses gemischten Volumes im Sicherheitsstil ist UNIX effektive Sicherheit. Das Volume verfügt über Sicherheit auf Storage-Ebene beim Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Verwandte Informationen

Anzeigen von Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes

Anzeigen von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Anzeige von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Sie können Informationen über die Datei- und Verzeichnissicherheit auf UNIX-Volumes im Sicherheitsstil anzeigen, einschließlich der Sicherheitsstile und der effektiven

Sicherheitsstile, welche Berechtigungen angewendet werden, sowie Informationen über UNIX-Besitzer und -Gruppen. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für die Datei oder das Verzeichnis angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- UNIX-Volumes und qtrees verwenden beim Bestimmen von Dateizugriffsrechten nur UNIX-Dateiberechtigungen, entweder Mode-Bits oder NFSv4-ACLs.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Verzeichnisse, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder für die Ausgabe der Eigentümer und der Gruppen in der ACL gelten nicht bei NFSv4-Sicherheitsdeskriptoren.

  Sie sind nur für NTFS-Sicherheitsdeskriptoren sinnvoll.

- Da die Sicherheit des Storage-Level Access Guard auf einem UNIX Volume oder qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die Sicherheit des Storage-Level Access Guard enthalten, der auf dem angegebenen Volume oder qtree im angewendet wird `-path` Parameter.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit mehr Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/home` In SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                 Vserver: vs1
                               File Path: /home
                       File Inode Number: 9590
                          Security Style: unix
                         Effective Style: unix
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 1
                          Unix Mode Bits: 700
                  Unix Mode Bits in Text: rwx------
                                    ACLs: -
```

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/home` In SVM vs1 als erweiterte Maske:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                 Vserver: vs1
                               File Path: /home
                       File Inode Number: 9590
                          Security Style: unix
                         Effective Style: unix
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: 0x10
                      ...0 .... .... .... = Offline
                      .... ..0. .... .... = Sparse
                      .... .... 0... .... = Normal
                      .... .... ..0. .... = Archive
                      .... .... ...1 .... = Directory
                      .... .... .... .0.. = System
                      .... .... .... ..0. = Hidden
                      .... .... .... ...0 = Read Only
                            Unix User Id: 0
                           Unix Group Id: 1
                          Unix Mode Bits: 700
                  Unix Mode Bits in Text: rwx------
                                    ACLs: -
```

Verwandte Informationen

Anzeigen von Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes

Anzeigen von Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart

Zeigt Informationen zu NTFS-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI an

Sie können Informationen zu NTFS-Audit-Richtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu Zugriffssteuerungslisten des Systems. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu validieren oder um Fehler bei der Prüfung von Problemen zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Ordnern angeben, deren Audit-Informationen angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Bei NTFS-Volumes und qtrees werden für Audit-Richtlinien nur NTFS-Systemzugriffssteuerungslisten (SACLs) verwendet.
- Dateien und Ordner in einem gemischten Security-Stil-Volume mit NTFS effektive Sicherheit können NTFS-Audit-Richtlinien auf sie angewendet werden.

  Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines gemischten Security-Volumes kann entweder UNIX oder NTFS effektive Sicherheit haben und möglicherweise NTFS SACLs enthalten.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume- oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, zeigt möglicherweise sowohl normale Datei als auch Ordner NFSv4 SACLs und Storage-Level Access Guard NTFS SACLs an.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS-effektiver Sicherheit besteht, zeigt die Ausgabe auch Informationen über Dynamic Access Control Aces an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Wenn Sicherheitsinformationen über Dateien und Ordner mit NTFS-effektiver Sicherheit angezeigt werden, enthalten UNIX-bezogene Ausgabefelder nur Informationen über die Berechtigung von UNIX-Dateien.

  NTFS-Dateien und -Ordner verwenden bei der Ermittlung der Zugriffsrechte auf Dateien nur NTFS-Dateiberechtigungen und Windows-Benutzer und -Gruppen.

- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige von Datei- und Verzeichnisaudits-Einstellungen mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Als detaillierte Liste	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Informationen zu den Überwachungsrichtlinien für den Pfad angezeigt `/corp` In SVM vs1. Der Pfad verfügt über NTFS effektive Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen ERFOLG als auch einen SACL-Eintrag FÜR ERFOLG/FEHLER.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         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
```

Im folgenden Beispiel werden die Informationen zu den Überwachungsrichtlinien für den Pfad angezeigt `/datavol1` In SVM vs1. Der Pfad enthält sowohl normale Datei- als auch Ordner-SACLs und Speicher-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         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:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Zeigt Informationen über die NFSv4-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI an

Sie können Informationen über NFSv4-Audit-Richtlinien auf FlexVol-Volumes über die

ONTAP-CLI anzeigen, einschließlich der Sicherheitsstile und des effektiven Sicherheitsstyles, der angewandten Berechtigungen und Informationen zu Systemzugriffssteuerungslisten (SACLs). Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu validieren oder um Fehler bei der Prüfung von Problemen zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Verzeichnissen angeben, deren Audit-Informationen angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- UNIX Volumes und qtrees im Sicherheitsstil verwenden ausschließlich NFSv4 SACLs für Prüfrichtlinien.
- Dateien und Verzeichnisse in einem gemischten Volume mit Sicherheitsstil, das sich im UNIX-Sicherheitsstil befinden, können NFSv4-Audit-Richtlinien auf sie anwenden.

  Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines gemischten Security-Volumes kann entweder UNIX oder NTFS effektive Sicherheit haben und darf NFSv4 SACLs nicht enthalten.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume- oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, zeigt möglicherweise sowohl normale NFSv4-Datei- und Verzeichnis-SACLs als auch Storage-Level Access Guard NTFS SACLs an.
- Da die Sicherheit des Storage-Level Access Guard auf einem UNIX Volume oder qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die Sicherheit des Storage-Level Access Guard enthalten, der auf dem angegebenen Volume oder qtree im angewendet wird `-path` Parameter.

Schritte

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/lab` In SVM vs1. Dieser UNIX-Pfad im Sicherheitsstil verfügt über eine NFSv4-SACL.

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

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Möglichkeiten zum Anzeigen von Informationen über Dateisicherheitsrichtlinien und Audit-Richtlinien

Mithilfe des Platzhalterzeichens (*) können Sie Informationen über Dateisicherheit und Audit-Richtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Root-Volume anzeigen.

Das Platzhalterzeichen (**) kann als letzte Unterkomponente eines bestimmten Verzeichnispfades verwendet werden, unter dem Sie Informationen zu allen Dateien und Verzeichnissen anzeigen möchten. Wenn Sie Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen „“** anzeigen möchten, müssen Sie den vollständigen Pfad innerhalb doppelter Anführungszeichen („``") angeben.

Beispiel

Mit dem folgenden Befehl mit dem Platzhalterzeichen werden die Informationen über alle Dateien und Verzeichnisse unter dem Pfad angezeigt `/1/` Von SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
             Security Style: mixed
            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:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
             Security Style: mixed
            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:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Mit dem folgenden Befehl werden Informationen zu einer Datei mit dem Namen „*“ unter dem Pfad angezeigt `/vol1/a` Von SVM vs1. Der Pfad ist in doppelte Anführungszeichen eingeschlossen (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Managen Sie NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf SVMs über die CLI

Managen Sie mithilfe der CLI-Übersicht NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf SVMs

Sie können die NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf Storage Virtual Machines (SVMs) über die Befehlszeilenschnittstelle managen.

Die NTFS-Dateisicherheitsrichtlinien und Audit-Richtlinien können von SMB-Clients oder über die CLI gemanagt werden. Die Verwendung der CLI zur Konfiguration von Dateisicherheitsrichtlinien und Audit-Richtlinien erfordert jedoch keinen Remote-Client zum Verwalten der Dateisicherheit. Die Verwendung der CLI kann den Zeitaufwand für das Anwenden der Sicherheit auf viele Dateien und Ordner mit einem einzigen Befehl erheblich reduzieren.

Sie können den Storage-Level Access Guard konfigurieren. Dies ist eine weitere Sicherheitsschicht, die von ONTAP auf SVM Volumes angewendet wird. Storage-Level Access Guard gilt für Zugriffe aller NAS-Protokolle auf das Storage-Objekt, auf das Storage-Level Access Guard angewendet wird.

Der Storage-Level Access Guard kann nur über die ONTAP-CLI konfiguriert und gemanagt werden. Sie können Storage-Level Access Guard-Einstellungen von SMB-Clients nicht verwalten. Wenn Sie darüber hinaus die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Storage-Level Access Guard nicht angezeigt. Die Sicherheit des Access Guard auf Storage-Ebene kann nicht von einem Client entzogen werden, selbst wenn ein System-

Administrator (Windows oder UNIX) dies durchführt. Daher bietet Storage-Level Access Guard eine zusätzliche Sicherheitsschicht für den Datenzugriff, die vom Storage-Administrator unabhängig festgelegt und gemanagt wird.

> Obwohl nur NTFS-Zugriffsberechtigungen für Storage-Level Access Guard unterstützt werden, kann ONTAP Sicherheitsprüfungen für den Zugriff über NFS auf Daten auf Volumes durchführen, auf denen Storage-Level Access Guard angewendet wird, wenn der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der das Volume besitzt, zuordnet.

NTFS Security-Volumes

Alle Dateien und Ordner in NTFS-SicherheitsVolumes und qtrees haben NTFS-basierte Sicherheitsoptionen. Sie können das verwenden `vserver security file-directory` Befehlsfamilie, um die folgenden Sicherheitstypen auf NTFS Security-Volumes zu implementieren:

- Dateiberechtigungen und Audit-Richtlinien für Dateien und Ordner im Volume
- Sicherheit des Storage-Level Access Guard auf Volumes

Unterschiedliche Volumes im Sicherheitsstil

Volumes und qtrees im gemischten Sicherheitsstil können einige Dateien und Ordner enthalten, die für UNIX effektive Sicherheit haben und UNIX-Dateiberechtigungen verwenden, entweder Mode-Bits oder NFSv4.x-ACLs und NFSv4.x-Audit-Richtlinien sowie einige Dateien und Ordner, die NTFS-effektive Sicherheit haben und NTFS-Dateiberechtigungen sowie Audit-Richtlinien verwenden. Sie können das verwenden `vserver security file-directory` Befehlsfamilie, um die folgenden Sicherheitsarten auf Daten im gemischten Sicherheitsstil anzuwenden:

- Dateiberechtigungen und Audit-Richtlinien für Dateien und Ordner mit NTFS effizientem Sicherheitsstil im gemischten Volume oder qtree
- Storage-Level Access Guard für Volumes mit NTFS und UNIX effektivem Sicherheitsstil

UNIX Volumes im Sicherheitsstil

UNIX Security-Volumes und qtrees enthalten Dateien und Ordner, die über effektive UNIX-Sicherheit verfügen (entweder Mode-Bits oder NFSv4.x ACLs). Wenn Sie den verwenden möchten, müssen Sie Folgendes beachten `vserver security file-directory` Befehlfamilie zur Implementierung der Sicherheit auf UNIX-Volumes im Sicherheitsstil:

- Der `vserver security file-directory` Mit der Befehlszeile kann nicht die UNIX-Dateisicherheitsrichtlinien und Audit-Richtlinien für UNIX-Volumes und -qtrees verwaltet werden.
- Sie können das verwenden `vserver security file-directory` Produktfamilie zur Konfiguration der Storage-Level Access Guard auf UNIX Volumes im Sicherheitsstil, vorausgesetzt, die SVM mit dem Ziel-Volume enthält einen CIFS-Server.

Verwandte Informationen

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

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

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

Sicherer Dateizugriff über Storage-Level Access Guard

Anwendungsfälle für die Verwendung der CLI zum Festlegen der Datei- und Ordnersicherheit

Da Sie die Sicherheit von Dateien und Ordnern lokal ohne Beteiligung eines Remote-Clients anwenden und verwalten können, können Sie die Zeit, die für die Festlegung von Massensicherheit auf einer großen Anzahl von Dateien oder Ordnern benötigt wird, deutlich verkürzen.

Die CLI bietet Ihnen die Möglichkeit, die Datei- und Ordnersicherheit in den folgenden Anwendungsfällen festzulegen:

- Dateispeicherung in großen Unternehmensumgebungen, z. B. File Storage in Home Directories
- Datenmigration
- Ändern der Windows-Domäne
- Standardisierung der Dateisicherheitsrichtlinien und Audit-Richtlinien in NTFS-Filesystemen

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

Wenn Sie die CLI zum Festlegen der Datei- und Ordnersicherheit verwenden, müssen Sie bestimmte Grenzwerte beachten.

- Der `vserver security file-directory` Die Befehlsfamilie unterstützt das Festlegen von NFSv4 ACLs nicht.

  NTFS-Sicherheitsdeskriptoren können nur auf NTFS-Dateien und -Ordner angewendet werden.

Anwenden von Sicherheitsdeskriptoren zur Anwendung der Datei- und Ordnersicherheit

Sicherheitsdeskriptoren enthalten die Zugriffssteuerungslisten, die bestimmen, welche Aktionen ein Benutzer für Dateien und Ordner ausführen kann, und welche Daten geprüft werden, wenn ein Benutzer auf Dateien und Ordner zugreift.

- **Berechtigungen**

  Berechtigungen werden vom Eigentümer eines Objekts erlaubt oder verweigert und bestimmen, welche Aktionen ein Objekt (Benutzer, Gruppen oder Computerobjekte) auf bestimmten Dateien oder Ordnern ausführen kann.

- **Sicherheitsdeskriptoren**

  Sicherheitsdeskriptoren sind Datenstrukturen, die Sicherheitsinformationen enthalten, die Berechtigungen definieren, die einer Datei oder einem Ordner zugeordnet sind.

- **Zugriffssteuerungslisten (ACLs)**

  Zugriffssteuerungslisten sind die Listen in einem Sicherheitsdeskriptor, die Informationen darüber enthalten, welche Aktionen Benutzer, Gruppen oder Computerobjekte in der Datei oder dem Ordner ausgeführt werden können, auf den der Sicherheitsdeskriptor angewendet wird. Der Sicherheitsdeskriptor

kann die folgenden zwei Typen von ACLs enthalten:

  - Frei wählbare Zugriffssteuerungslisten
  - Systemzugriffssteuerungslisten (SACLs)

- **Ermessenslisten für die Zugriffskontrolle (DACLs)**

  DACLs enthalten die Liste von SIDS für Benutzer, Gruppen und Computerobjekte, die Zugriff auf Aktionen in Dateien oder Ordnern haben oder deren Zugriff verweigert wird. DACLs enthalten mindestens null Aces (Access Control Entries).

- **System Access Control Lists (SACLs)**

  SACLs enthalten die Liste von SCDs für die Benutzer, Gruppen und Computerobjekte, für die erfolgreiche oder fehlgeschlagene Überwachungsereignisse protokolliert werden. SACLs enthalten mindestens Null Zugangskontrolleinträge (Aces).

- * Access Control-Einträge (Asse)*

  Aces sind individuelle Einträge in DACLs oder SACLs:

  - Ein Eintrag für die DACL-Zugriffssteuerung legt die Zugriffsrechte fest, die für bestimmte Benutzer, Gruppen oder Computerobjekte zulässig oder verweigert werden.
  - Ein Eintrag zur SACL-Zugriffssteuerung gibt die Erfolg- oder Fehlerereignisse an, die bei der Prüfung der angegebenen Aktionen, die von bestimmten Benutzern, Gruppen oder Computerobjekten durchgeführt werden, protokolliert werden sollen.

- **Erben der Erlaubnis**

  Die Berechtigungsvererbung beschreibt, wie in Sicherheitsdeskriptoren definierte Berechtigungen aus einem übergeordneten Objekt auf ein Objekt übertragen werden. Nur vererbbare Berechtigungen werden von untergeordneten Objekten übernommen. Wenn Sie Berechtigungen für das übergeordnete Objekt festlegen, können Sie entscheiden, ob Ordner, Unterordner und Dateien sie mit „`Apply to`" erben können `this-folder`, `sub-folders`, Und `Files``".

Verwandte Informationen

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

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

Richtlinien zum Anwenden von Dateiverzeichnisrichtlinien, die lokale Benutzer oder Gruppen auf dem SVM Disaster-Recovery-Ziel verwenden

Es gibt bestimmte Richtlinien, die Sie beachten müssen, bevor Sie Dateiverzeichnisrichtlinien auf dem SVM-Disaster-Recovery-Ziel (Storage Virtual Machine) in einer ID-Verwerfen-Konfiguration anwenden, wenn die Konfiguration Ihrer Dateiverzeichnisrichtlinie lokale Benutzer oder Gruppen im Sicherheitsdeskriptor oder in den DACL- oder SACL-Einträgen verwendet.

Sie können eine Disaster-Recovery-Konfiguration für eine SVM konfigurieren, bei der die Quell-SVM auf dem Quellcluster die Daten und Konfigurationen von der Quell-SVM auf eine Ziel-SVM auf einem Ziel-Cluster repliziert.

Sie können einen der zwei Arten von Disaster-Recovery für SVM einrichten:

- Identität wurde erhalten

  Mit dieser Konfiguration wird die Identität der SVM und des CIFS-Servers beibehalten.

- Identität verworfen

  Mit dieser Konfiguration wird die Identität der SVM und des CIFS-Servers nicht erhalten. In diesem Szenario unterscheidet sich der Name der SVM und der CIFS-Server auf der Ziel-SVM von der SVM und dem CIFS-Servernamen auf der Quell-SVM.

Richtlinien für identitätsentworfene Konfigurationen

Bei einer Konfiguration mit einer über die Identität ausgelegten Identität muss für eine SVM-Quelle, die lokale Benutzer-, Gruppen- und Berechtigungskonfigurationen enthält, der Name der lokalen Domäne (lokaler CIFS-Servername) geändert werden, um mit dem CIFS-Servernamen auf dem SVM-Ziel überein. Wenn beispielsweise der Name der Quell-SVM „`vs1`“ und der Name des CIFS-Servers „`CIFS1`“ lautet und der Ziel-SVM-Name „`vs1_dst`“ und der CIFS-Servername „`CIFS1_DST`“ lautet, wird der lokale Domänenname für einen lokalen Benutzer mit dem Namen „`CIFS1\user1`“ automatisch in „`CIFS1_DST\SVM`“ `auf dem Ziel geändert: User1` SVM „user1“ auf dem Ziel: „User“.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Auch wenn lokale Benutzer- und Gruppennamen in den lokalen Benutzer- und Gruppendatenbanken automatisch geändert werden, werden lokale Benutzer oder Gruppennamen in den Dateiverzeichnisrichtlinien-Konfigurationen nicht automatisch geändert (Richtlinien, die in der CLI unter Verwendung der konfiguriert sind `vserver security file-directory` Befehlsfamilie).

Beispiel: Für „`vs1`“, wenn Sie einen DACL-Eintrag für den konfiguriert haben `-account` Der Parameter ist auf „`CIFS1\user1`“ gesetzt. Die Einstellung wird auf der Ziel-SVM nicht automatisch geändert, um den CIFS-Servernamen des Ziels anzugeben.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Sie müssen den verwenden `vserver security file-directory modify` Befehle zum manuellen Ändern des CIFS-Servernamens zum Ziel-CIFS-Servernamen.

Komponenten der Dateiverzeichnisrichtlinie, die Kontoparameter enthalten

Es gibt drei Konfigurationskomponenten für die Dateiverzeichnisrichtlinie, die Parametereinstellungen verwenden können, die lokale Benutzer oder Gruppen enthalten können:

- Sicherheitsdeskriptor

  Sie können optional den Besitzer des Sicherheitsdeskriptors und die primäre Gruppe des Besitzers des Sicherheitsdeskriptors angeben. Wenn beim Sicherheitsdeskriptor ein lokaler Benutzer oder eine lokale Gruppe für die Einträge in den Inhabern und der primären Gruppe verwendet wird, müssen Sie den Sicherheitsdeskriptor ändern, um im Kontonamen die Ziel-SVM zu verwenden. Sie können das verwenden `vserver security file-directory ntfs modify` Befehl, um alle erforderlichen Änderungen an den Kontonamen vorzunehmen.

- DACL-Einträge

  Jeder DACL-Eintrag muss einem Konto zugeordnet sein. Sie müssen alle DACLs ändern, die lokale Benutzer- oder Gruppenkonten verwenden, um den Ziel-SVM-Namen zu verwenden. Da Sie den Kontonamen für vorhandene DACL-Einträge nicht ändern können, müssen Sie alle DACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren entfernen, neue DACL-Einträge mit den korrigierten Zielkontonamen erstellen und diese neuen DACL-Einträge mit den entsprechenden Sicherheitsdeskriptoren verknüpfen.

- SACL-Einträge

  Jeder SACL-Eintrag muss einem Konto zugeordnet sein. Sie müssen alle SACLs ändern, die lokale

Benutzer- oder Gruppenkonten verwenden, um den Ziel-SVM-Namen zu verwenden. Da Sie den Kontonamen für vorhandene SACL-Einträge nicht ändern können, müssen Sie alle SACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren entfernen, neue SACL-Einträge mit den korrigierten Zielkontonamen erstellen und diese neuen SACL-Einträge mit den entsprechenden Sicherheitsdeskriptoren verknüpfen.

Vor der Anwendung der Richtlinie müssen Sie alle erforderlichen Änderungen an lokalen Benutzern oder Gruppen vornehmen, die in der Konfiguration der Dateiverzeichnisrichtlinien verwendet werden. Andernfalls schlägt der Auftrag zum Anwenden fehl.

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

Erstellen Sie einen NTFS-Sicherheitsdeskriptor

Das Erstellen eines NTFS-Sicherheitsdeskriptors (Dateisicherheitsrichtlinie) ist der erste Schritt bei der Konfiguration und Anwendung von NTFS-Zugriffssteuerungslisten (NTFS Access Control Lists, ACLs) auf Dateien und Ordner innerhalb der Storage Virtual Machines (SVMs). Sie können den Sicherheitsdeskriptor in einer Richtlinienaufgabe dem Datei- oder Ordnerpfad zuordnen.

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.

Fügen Sie dem NTFS-Sicherheitsdeskriptor NTFS-DACL-Zugriffssteuerungseinträge hinzu

Das Hinzufügen von DACL (Ermessensliste für die Zugriffssteuerung) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Konfiguration und Anwendung von NTFS-ACLs auf eine Datei oder einen Ordner. Jeder Eintrag identifiziert, welches Objekt erlaubt oder verweigert wird, und definiert, was das Objekt für die im ACE definierten Dateien oder Ordner tun kann oder nicht.

Über diese Aufgabe

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

Wenn der Sicherheitsdeskriptor eine DACL enthält, die Asse enthält, fügt der Befehl den neuen ACE zum DACL hinzu. Wenn der Sicherheitsdeskriptor keine DACL enthält, erstellt der Befehl die DACL und fügt den neuen ACE hinzu.

Sie können optional DACL-Einträge anpassen, indem Sie angeben, welche Rechte Sie für das in angegebene Konto zulassen oder verweigern 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 DACL-Eintrag angeben, werden standardmäßig die Rechte auf festgelegt `Full Control`.

Sie können optional DACL-Einträge anpassen, indem Sie festlegen, wie Vererbung angewendet wird.

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

Schritte

1. Hinzufügen eines DACL-Eintrags zu einem Sicherheitsdeskriptor: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

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

2. Überprüfen Sie, ob der DACL-Eintrag korrekt ist: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

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

```
                    Vserver: vs1
         Security Descriptor Name: sd1
                   Allow or Deny: deny
             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 Dateisicherheitsrichtlinie für SVMs ist der dritte Schritt beim Konfigurieren und Anwenden 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 SVM zuweisen (die NTFS Security-Volumes oder Volumes im gemischten Sicherheitsstil enthält).

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.

Beim Hinzufügen von Aufgaben zu Sicherheitsrichtlinien müssen Sie die folgenden vier erforderlichen Parameter angeben:

- SVM-Name
- Name der Richtlinie
- Pfad
- Sicherheitsdeskriptor, der mit dem Pfad verknüpft wird

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

Der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner ist die Anwendung einer Dateisicherheitsrichtlinie auf SVMs.

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).

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

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 angewendete Dateisicherheit

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

Über diese Aufgabe

Sie müssen den Namen der SVM angeben, die die Daten sowie den Pfad zu der Datei und den Ordnern enthält, auf denen Sie die Sicherheitseinstellungen überprüfen möchten. Sie können das optionale verwenden `-expand-mask` Parameter zum Anzeigen detaillierter Informationen zu den Sicherheitseinstellungen.

Schritt

1. Sicherheitseinstellungen für Datei und Ordner anzeigen: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true`

```
          Vserver: vs1
               File Path: /data/engineering
       File Inode Number: 5544
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
```

```
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
```

```
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

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

Der letzte Schritt bei der Erstellung und Anwendung von NTFS-ACLs auf Dateien oder Ordner ist die Anwendung einer Audit-Richtlinie auf SVMs.

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).

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

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
```

Überlegungen bei der Verwaltung von Aufgaben mit Sicherheitsrichtlinien

Wenn ein Job für die Sicherheitsrichtlinien vorhanden ist, können Sie diese Sicherheitsrichtlinie oder die Aufgaben, die dieser Richtlinie zugewiesen sind, nicht ändern. Sie sollten unter welchen Bedingungen Sie die Sicherheitsrichtlinien ändern können oder können, damit alle Änderungsversuche erfolgreich sind. Änderungen an der Richtlinie umfassen das Hinzufügen, Entfernen oder Ändern von Aufgaben, die der Richtlinie zugewiesen sind, sowie das Löschen oder Ändern der Richtlinie.

Sie können eine Sicherheitsrichtlinie oder eine Aufgabe, die dieser Richtlinie zugewiesen ist, nicht ändern, wenn ein Job für diese Richtlinie existiert und sich dieser Job in den folgenden Status befindet:

- Der Job wird ausgeführt oder wird ausgeführt.
- Der Job wurde angehalten.
- Der Job wird wieder aufgenommen und befindet sich im laufenden Zustand.
- Wenn der Job auf ein Failover auf einen anderen Node wartet.

Wenn ein Job für eine Sicherheitsrichtlinie vorhanden ist, können Sie unter folgenden Umständen diese Sicherheitsrichtlinie oder eine dieser Richtlinie zugewiesene Aufgabe erfolgreich ändern:

- Der Richtlinienjob wird angehalten.
- Der Richtlinienjob wurde erfolgreich abgeschlossen.

Befehle zum Verwalten von NTFS-Sicherheitsdeskriptoren

Für das Management von Sicherheitsdeskriptoren gibt es bestimmte ONTAP-Befehle. Sie können Informationen zu Sicherheitsdeskriptoren erstellen, ändern, löschen und anzeigen.

Ihr Ziel ist	Befehl
NTFS-Sicherheitsdeskriptoren erstellen	`vserver security file-directory ntfs create`
Vorhandene NTFS-Sicherheitsdeskriptoren ändern	`vserver security file-directory ntfs modify`
Informationen zu vorhandenen NTFS-Sicherheitsdeskriptoren anzeigen	`vserver security file-directory ntfs show`
Löschen Sie NTFS-Sicherheitsdeskriptoren	`vserver security file-directory ntfs delete`

Siehe die man-Pages für die `vserver security file-directory ntfs` Befehle für weitere Informationen.

Befehle zum Verwalten von NTFS-DACL-Zugriffssteuerungseinträgen

Es gibt bestimmte ONTAP-Befehle zur Verwaltung von DACL Access Control Entries (Aces). Sie können Aces zu NTFS DACLs jederzeit hinzufügen. Sie können auch vorhandene NTFS-DACLs verwalten, indem Sie Informationen über Aces in DACLs ändern, löschen und anzeigen.

Ihr Ziel ist	Befehl
Erstellen Sie Aces und fügen Sie sie zu NTFS-DACLs hinzu	`vserver security file-directory ntfs dacl add`
Vorhandene Asse in NTFS-DACLs ändern	`vserver security file-directory ntfs dacl modify`
Informationen über vorhandene Asse in NTFS-DACLs anzeigen	`vserver security file-directory ntfs dacl show`
Entfernen Sie vorhandene Aces aus NTFS-DACLs	`vserver security file-directory ntfs dacl remove`

Siehe die man-Pages für die `vserver security file-directory ntfs dacl` Befehle für weitere Informationen.

Befehle zum Verwalten von NTFS SACL-Zugriffssteuerungseinträgen

Es gibt bestimmte ONTAP-Befehle zur Verwaltung von SACL Access Control Einträgen (Aces). Sie können Aces zu NTFS SACLs jederzeit hinzufügen. Sie können auch vorhandene NTFS-SACLs verwalten, indem Sie Informationen über Asse in SACLs ändern, löschen und anzeigen.

Ihr Ziel ist	Befehl
Asse erstellen und zu NTFS SACLs hinzufügen	`vserver security file-directory ntfs sacl add`
Vorhandene Asse in NTFS SACLs ändern	`vserver security file-directory ntfs sacl modify`
Informationen über vorhandene Asse in NTFS SACLs anzeigen	`vserver security file-directory ntfs sacl show`
Entfernen Sie vorhandene Asse aus NTFS SACLs	`vserver security file-directory ntfs sacl remove`

Siehe die man-Pages für die `vserver security file-directory ntfs sacl` Befehle für weitere Informationen.

Befehle zum Verwalten von Sicherheitsrichtlinien

Zum Management von Sicherheitsrichtlinien gibt es bestimmte ONTAP-Befehle. Sie können Informationen zu Richtlinien anzeigen und Richtlinien löschen. Sie können eine Sicherheitsrichtlinie nicht ändern.

Ihr Ziel ist	Befehl
Erstellen von Sicherheitsrichtlinien	`vserver security file-directory policy create`
Zeigt Informationen zu Sicherheitsrichtlinien an	`vserver security file-directory policy show`
Sicherheitsrichtlinien löschen	`vserver security file-directory policy delete`

Siehe die man-Pages für die `vserver security file-directory policy` Befehle für weitere Informationen.

Befehle zum Verwalten von Aufgaben für Sicherheitsrichtlinien

Es gibt ONTAP-Befehle zum Hinzufügen, Ändern, Entfernen und Anzeigen von Informationen zu Aufgaben der Sicherheitsrichtlinien.

Ihr Ziel ist	Befehl
Aufgaben für Sicherheitsrichtlinien hinzufügen	`vserver security file-directory policy task add`
Aufgaben für Sicherheitsrichtlinien ändern	`vserver security file-directory policy task modify`
Zeigt Informationen zu Aufgaben der Sicherheitsrichtlinien an	`vserver security file-directory policy task show`
Aufgaben für Sicherheitsrichtlinien entfernen	`vserver security file-directory policy task remove`

Siehe die man-Pages für die `vserver security file-directory policy task` Befehle für weitere Informationen.

Befehle zum Verwalten von Aufgaben für Sicherheitsrichtlinien

Es gibt ONTAP-Befehle, mit denen Informationen zu Jobs mit Sicherheitsrichtlinien angehalten, fortgesetzt, angehalten und angezeigt werden können.

Ihr Ziel ist	Befehl
Unterbrechen Sie Aufgaben für Sicherheitsrichtlinien	`vserver security file-directory job pause -vserver vserver_name -id integer`
Aufgaben für Sicherheitsrichtlinien wieder aufnehmen	`vserver security file-directory job resume -vserver vserver_name -id integer`
Informationen zu Jobs mit Sicherheitsrichtlinie anzeigen	`vserver security file-directory job show -vserver vserver_name` Mit diesem Befehl können Sie die Job-ID eines Jobs bestimmen.
Stoppen Sie Jobs für Sicherheitsrichtlinien	`vserver security file-directory job stop -vserver vserver_name -id integer`

Siehe die man-Pages für die `vserver security file-directory job` Befehle für weitere Informationen.

Konfigurieren Sie den Metadaten-Cache für SMB-Freigaben

Funktionsweise des SMB-Metadaten-Caching

Durch das Metadaten-Caching von Dateiattributen auf SMB 1.0 Clients können Sie schneller auf Datei- und Ordnerattribute zugreifen. Sie können das Attribut-Caching auf der Basis der einzelnen Freigaben aktivieren oder deaktivieren. Sie können auch die Live-Zeit für zwischengespeicherte Einträge konfigurieren, wenn das Metadaten-Caching aktiviert ist. Das Konfigurieren des Metadaten-Caching ist nicht erforderlich, wenn Clients eine Verbindung zu Freigaben über SMB 2.x oder SMB 3.0 herstellen.

Wenn diese Option aktiviert ist, speichert der SMB Metadaten-Cache Pfad- und Dateiattributdaten für eine begrenzte Zeit. So kann die SMB-Performance für SMB 1.0-Clients mit gängigen Workloads gesteigert werden.

Bei bestimmten Aufgaben erzeugt SMB eine beträchtliche Menge an Datenverkehr, die mehrere identische Abfragen für Pfad- und Dateimetadaten umfassen kann. Es lässt sich die Anzahl redundanter Abfragen reduzieren und die Performance für SMB 1.0 Clients verbessern, indem stattdessen beim SMB-MetadatenCaching Informationen aus dem Cache abgerufen werden.

> Obwohl es unwahrscheinlich ist, ist es möglich, dass der Metadaten-Cache veraltete Informationen für SMB 1.0 Clients bereitstellen kann. Wenn sich Ihre Umgebung dieses Risiko nicht leisten kann, sollten Sie diese Funktion nicht aktivieren.

Aktivieren des SMB-Metadaten-Caches

Durch die Aktivierung des SMB Metadaten-Caches können Sie die Performance von SMB 1.0 Clients verbessern. Standardmäßig ist das Caching von SMB-Metadaten deaktiviert.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie SMB-Metadaten-Caching beim Erstellen einer Freigabe	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
SMB-Metadaten-Caching bei einer vorhandenen Freigabe aktivieren	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

Verwandte Informationen

Konfigurieren der Nutzungsdauer von SMB-Metadatencache-Einträgen

Hinzufügen oder Entfernen von Share-Eigenschaften für eine vorhandene SMB-Freigabe

Konfigurieren Sie die Nutzungsdauer von SMB-Metadaten-Cache-Einträgen

Sie können die Nutzungsdauer von SMB-Metadaten-Cache-Einträgen konfigurieren, um die Performance des SMB-Metadaten-Caches in Ihrer Umgebung zu optimieren. Der Standardwert beträgt 10 Sekunden.

Bevor Sie beginnen

Sie müssen die SMB-Metadaten-Cache-Funktion aktiviert haben. Wenn das SMB-Metadaten-Caching nicht aktiviert ist, wird die TTL-Einstellung des SMB-Caches nicht verwendet.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Wenn Sie die Lebensdauer von SMB-Metadaten-Cache-Einträgen konfigurieren möchten, wenn Sie…	Geben Sie den Befehl ein…
Erstellen Sie eine Freigabe	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
Vorhandene Freigabe ändern	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

Sie können zusätzliche Optionen und Eigenschaften für die Freigabkonfiguration beim Erstellen oder Ändern von Freigaben festlegen. Weitere Informationen finden Sie auf den man-Pages.

Verwalten von Dateisperren

Über die Dateisperrung zwischen Protokollen

Die Dateisperrung wird von Client-Anwendungen verwendet, um zu verhindern, dass ein Benutzer auf eine Datei zugreift, die zuvor von einem anderen Benutzer geöffnet wurde. Wie ONTAP Dateien sperrt, hängt vom Protokoll des Clients ab.

Wenn es sich bei dem Client um einen NFS-Client handelt, sind Locks Advisory. Wenn es sich bei dem Client um einen SMB-Client handelt, sind Locks obligatorisch.

Aufgrund der Unterschiede zwischen den Dateisperren für NFS und SMB kann ein NFS-Client nicht auf eine Datei zugreifen, die zuvor von einer SMB-Applikation geöffnet wurde.

Die folgende Meldung tritt auf, wenn ein NFS-Client versucht, auf eine Datei zuzugreifen, die von einer SMB-Applikation gesperrt wurde:

- In gemischten oder NTFS-Volumes führen Dateimanipulation-Vorgänge wie `rm`, `rmdir`, und `mv` Fehler der NFS-Applikation kann auftreten.
- Lese- und Schreibvorgänge für NFS werden vom SMB Deny-read- bzw. Deny-Write-Open-Modus verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei durch einen exklusiven SMB-Bytelock gesperrt ist.
- Link Aufheben
  - Für NTFS-Dateisysteme werden SMB- und CIFS-Löschvorgänge unterstützt.

    Die Datei wird nach dem letzten Schließen entfernt.
  - Vorgänge zum Aufheben der Verknüpfung von NFS werden nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind und der Vorgang Letztes Löschen bei Schließen für NFS nicht unterstützt wird.
  - Für UNIX-Dateisysteme wird der Aufheben der Verknüpfung unterstützt.

    Dies wird unterstützt, da NFS- und UNIX-Semantik erforderlich sind.
- Umbenennen
  - Bei NTFS-Dateisystemen kann die Zieldatei umbenannt werden, wenn die Zieldatei von SMB oder CIFS geöffnet wird.
  - NFS-Umbenennung wird nicht unterstützt.

    Es wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind.

In UNIX-Volumes im Sicherheitsstil ignorieren NFS den SMB-Sperrstatus und erlauben den Zugriff auf die Datei. Alle anderen NFS-Vorgänge auf UNIX Volumes im Sicherheitsstil sorgen für den SMB-Lock-Status.

Wie ONTAP schreibgeschützte Bits behandelt

Das schreibgeschützte Bit wird auf Datei-für-Datei-Basis gesetzt, um zu reflektieren, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients, die Windows verwenden, können einen schreibgeschützten Bit pro Datei festlegen. NFS-Clients legen kein Leserbit pro Datei fest, da NFS-Clients über keine Protokollvorgänge verfügen, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann ein schreibgeschütztes Bit auf einer Datei festlegen, wenn ein SMB-Client, der Windows verwendet, diese Datei erstellt. ONTAP kann auch ein schreibgeschütztes Bit festlegen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Für einige Software, die von NFS-Clients und SMB-Clients verwendet wird, ist die Aktivierung des Read-Only-Bits erforderlich.

Damit ONTAP die entsprechenden Lese- und Schreibberechtigungen auf eine von NFS Clients und SMB Clients gemeinsam genutzte Datei vorhält, behandelt es das schreibgeschützte Bit gemäß den folgenden Regeln:

- NFS behandelt jede Datei mit aktiviertem Read-Only-Bit, als ob keine Write-Berechtigungsbits aktiviert sind.

- Wenn ein NFS-Client alle Write-Berechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert wurde, aktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungs-Bit aktiviert, deaktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein NFS-Client versucht, Berechtigungen für die Datei zu ermitteln, werden die Berechtigungsbits für die Datei nicht an den NFS-Client gesendet. Stattdessen sendet ONTAP die Berechtigungsbits an den NFS-Client mit maskierten Schreibberechtigungs-Bits.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein SMB-Client das schreibgeschützte Bit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien mit aktiviertem Read-Only-Bit sind nur als Root beschreibbar.

> Änderungen an Dateiberechtigungen wirken sich unmittelbar auf SMB-Clients aus, wirken sich jedoch möglicherweise nicht unmittelbar auf NFS-Clients aus, wenn der NFS-Client das Caching von Attributen ermöglicht.

Wie unterscheidet sich ONTAP von Windows bei der Handhabung von Sperren auf Share-Pfad-Komponenten

Im Gegensatz zu Windows sperrt ONTAP nicht jede Komponente des Pfads zu einer geöffneten Datei, während die Datei geöffnet ist. Dieses Verhalten wirkt sich auch auf die SMB-Freigabungspfade aus.

Da ONTAP nicht jede Komponente des Pfads sperrt, ist es möglich, eine Pfadkomponente über der offenen Datei oder Freigabe umzubenennen, was zu Problemen für bestimmte Anwendungen führen kann oder dass der Freigabepfad in der SMB-Konfiguration ungültig ist. Dies kann dazu führen, dass der Share nicht zugänglich ist.

Um Probleme zu vermeiden, die durch die Umbenennung von Pfadkomponenten verursacht werden, können Sie Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Informationen zu Sperren anzeigen

Sie können Informationen über die aktuellen Dateisperren anzeigen, einschließlich der Arten von Sperren und des Sperrstatus, Informationen über Byte-Range-Sperren, Sharlock-Modi, Delegiertersicherungen und opportunistische Sperren sowie darüber, ob Sperren mit langlebigen oder dauerhaften Griffen geöffnet werden.

Über diese Aufgabe

Die Client-IP-Adresse kann nicht für Sperren angezeigt werden, die über NFSv4 oder NFSv4.1 eingerichtet wurden.

Standardmäßig werden mit dem Befehl Informationen zu allen Sperren angezeigt. Mit den Befehlsparametern können Informationen über Sperren für eine bestimmte Storage Virtual Machine (SVM) angezeigt oder die Ausgabe des Befehls nach anderen Kriterien gefiltert werden.

Der `vserver locks show` Befehl zeigt Informationen zu vier Arten von Sperren an:

- Byte-Bereich-Locks, die nur einen Teil einer Datei sperren.
- Sperren freigeben, die geöffnete Dateien sperren
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Caching des Clients über NFSv4.x steuern

Durch die Angabe optionaler Parameter können Sie wichtige Informationen zu jedem Sperrtyp ermitteln. Weitere Informationen finden Sie auf der man-Page des Befehls.

Schritt

1. Zeigen Sie Informationen über Sperren mithilfe des an `vserver locks show` Befehl.

Beispiele

Im folgenden Beispiel werden zusammenfassende Informationen für eine NFSv4-Sperre auf einer Datei mit dem Pfad angezeigt `/vol1/file1`. Der Zugriffsmodus für sharlock ist write-Deny_none, und die Sperre wurde mit der Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1                lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                          delegation  -
               Delegation Type: write
```

Das folgende Beispiel zeigt detaillierte oplock- und Share-Informationen über die SMB-Sperre auf einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird auf der Datei mit einem Zugriffsmodus für die Freigabesperre von write-Deny_none einem Client mit einer IP-Adresse von 10.3.1.3 gewährt. Ein Lease Oplock wird mit einem Batch-Oplock-Niveau gewährt:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
```

```
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Sperren

Wenn Dateisperren den Client-Zugriff auf Dateien verhindern, können Sie Informationen zu derzeit gespeicherten Sperren anzeigen und bestimmte Sperren anschließend unterbrechen. Beispiele für Szenarien, in denen Sie Sperren benötigen, sind Debugging-Anwendungen.

Über diese Aufgabe

Der `vserver locks break` Befehl ist nur auf der erweiterten Berechtigungsebene und höher verfügbar. Die man-Page für den Befehl enthält detaillierte Informationen.

Schritte

1. Um die Informationen zu finden, die Sie benötigen, um eine Sperre zu brechen, verwenden Sie die `vserver locks show` Befehl.

   Die man-Page für den Befehl enthält detaillierte Informationen.

2. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
3. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie eine Sperre brechen möchten, indem Sie…	Geben Sie den Befehl ein…
Der Name der SVM, der Name des Volumes, der LIF-Name und der Dateipfad	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
Die Lock-ID	`vserver locks break -lockid UUID`

4. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Überwachen Sie die SMB-Aktivitäten

Zeigt SMB-Sitzungsinformationen an

Sie können Informationen zu festgelegten SMB-Sitzungen anzeigen, einschließlich der SMB-Verbindung und der Sitzungs-ID sowie der IP-Adresse der Workstation über die Sitzung. Sie können Informationen zur SMB-Protokollversion der Sitzung und zum kontinuierlich verfügbaren Sicherungslevel anzeigen, sodass Sie leichter feststellen können, ob die Session den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen zu allen Sitzungen Ihrer SVM in zusammengefassener Form anzeigen. In vielen Fällen ist jedoch die Menge der zurückgegebenen Ausgabe groß. Sie können die in der Ausgabe angezeigten Informationen anpassen, indem Sie optionale Parameter angeben:

- Sie können das optionale verwenden `-fields` Parameter, um die Ausgabe der ausgewählten Felder anzuzeigen.

  Sie können eingeben `-fields ?` Um zu bestimmen, welche Felder Sie verwenden können.

- Sie können das verwenden `-instance` Parameter zum Anzeigen detaillierter Informationen zu festgelegten SMB-Sitzungen.
- Sie können das verwenden `-fields` Parameter oder der `-instance` Parameter allein oder in Kombination mit anderen optionalen Parametern.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
Für alle Sitzungen auf der SVM in Übersichtsform	`vserver cifs session show -vserver vserver_name`
Bei einer angegebenen Verbindungs-ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
Von einer angegebenen IP-Adresse der Workstation	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Auf einer angegebenen LIF-IP-Adresse	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Auf einem angegebenen Node	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	Von einem angegebenen Windows-Benutzer
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Mit einem angegebenen Authentifizierungsmechanismus
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Mit einer angegebenen Protokollversion	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== Kontinuierlich verfügbarer Schutz und SMB MultiChannel sind nur für SMB 3.0 und höhere Sitzungen verfügbar. Um ihren Status bei allen qualifizierenden Sitzungen anzuzeigen, sollten Sie diesen Parameter angeben, auf den der Wert festgelegt ist `SMB3` Oder höher. ====

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
Mit einem festgelegten Maß an kontinuierlich verfügbarem Schutz	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Wenn der Status „kontinuierlich verfügbar“ lautet `Partial`, Das bedeutet, dass die Sitzung mindestens eine offene kontinuierlich verfügbare Datei enthält, aber die Sitzung hat einige Dateien, die nicht geöffnet sind mit kontinuierlich verfügbaren Schutz. Sie können das verwenden `vserver cifs sessions file show` Befehl zum Bestimmen, welche Dateien in der festgelegten Sitzung nicht geöffnet sind, mit kontinuierlich verfügbarem Schutz. ====
Mit einem angegebenen SMB Signing Session Status	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Beispiele

Mit dem folgenden Befehl werden die Sitzungsinformationen für die Sitzungen auf SVM vs1 angezeigt, die von einer Workstation mit der IP-Adresse 10.1.1.1 eingerichtet wurden:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

Mit dem folgenden Befehl werden ausführliche Sitzungsinformationen für Sitzungen mit kontinuierlich verfügbarem Schutz für SVM vs1 angezeigt. Die Verbindung wurde über das Domain-Konto hergestellt.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Mit dem folgenden Befehl werden Sitzungsinformationen zu einer Sitzung mit SMB 3.0 und SMB Multichannel in SVM vs1 angezeigt. Im Beispiel hat der Benutzer über einen SMB 3.0-fähigen Client mithilfe der LIF-IP-Adresse eine Verbindung zu dieser Freigabe hergestellt. Daher wurde der Authentifizierungsmechanismus standardmäßig auf NTLMv2 festgelegt. Die Verbindung muss über die Kerberos-Authentifizierung hergestellt werden, um eine Verbindung mit kontinuierlich verfügbarem Schutz herzustellen.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Verwandte Informationen

Anzeigen von Informationen über geöffnete SMB-Dateien

Zeigt Informationen zu geöffneten SMB-Dateien an

Sie können Informationen zu offenen SMB-Dateien anzeigen, einschließlich SMB-Verbindung und Session-ID, Hosting-Volume, Share-Name und Freigabepfad. Sie können Informationen über den kontinuierlich verfügbaren Sicherungsgrad einer Datei anzeigen. Dies ist hilfreich bei der Feststellung, ob sich eine offene Datei in einem Zustand befindet, der den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen über offene Dateien in einer festgelegten SMB-Sitzung anzeigen. Die angezeigten Informationen sind nützlich, wenn Sie SMB-Sitzungsinformationen für bestimmte Dateien innerhalb einer SMB-Sitzung bestimmen müssen.

Wenn Sie zum Beispiel über eine SMB-Sitzung verfügen, bei der einige der offenen Dateien mit kontinuierlich verfügbarem Schutz geöffnet sind und einige nicht mit kontinuierlich verfügbarem Schutz geöffnet sind (der Wert für das `-continuously-available` Feld in `vserver cifs session show` Befehlsausgabe ist `Partial`Mit diesem Befehl können Sie bestimmen, welche Dateien nicht ständig verfügbar sind.

Mit der können Sie Informationen zu allen offenen Dateien in festgelegten SMB-Sitzungen auf Storage Virtual Machines (SVMs) in zusammengefassener Form anzeigen `vserver cifs session file show` Befehl

ohne optionale Parameter.

In vielen Fällen ist jedoch die zurückgegebene Menge an Output groß. Sie können die in der Ausgabe angezeigten Informationen durch optionale Parameter anpassen. Dies kann hilfreich sein, wenn Sie Informationen nur für einen kleinen Teil der offenen Dateien anzeigen möchten.

- Sie können das optionale verwenden `-fields` Parameter zum Anzeigen der Ausgabe in den ausgewählten Feldern.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

- Sie können das verwenden `-instance` Parameter zum Anzeigen detaillierter Informationen zu offenen SMB-Dateien.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie öffnen SMB-Dateien anzeigen möchten…	**Geben Sie den folgenden Befehl ein…**
Auf der SVM in Übersichtsform	`vserver cifs session file show -vserver vserver_name`
Auf einem angegebenen Node	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	Für eine angegebene Datei-ID
`vserver cifs session file show -vserver vserver_name -file-id integer`	Für eine angegebene SMB-Verbindungs-ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Für eine angegebene SMB-Session-ID
`vserver cifs session file show -vserver vserver_name -session-id integer`	Auf dem angegebenen Hosting-Aggregat
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	Auf dem angegebenen Volume

Wenn Sie öffnen SMB-Dateien anzeigen möchten…	Geben Sie den folgenden Befehl ein…
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	In der angegebenen SMB-Freigabe
`vserver cifs session file show -vserver vserver_name -share share_name`	Auf dem angegebenen SMB-Pfad
`vserver cifs session file show -vserver vserver_name -path path`	Mit der angegebenen Stufe des kontinuierlichen verfügbaren Schutzes
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Wenn der Status „kontinuierlich verfügbar“ lautet `No`, Das heißt, diese offenen Dateien können nicht unterbrechungsfrei nach Takeover und Giveback wiederhergestellt werden. Sie sind auch bei der allgemeinen Aggregatverschiebung zwischen den Partnern in einer Hochverfügbarkeitbeziehung nicht wiederherstellbar. ====
Mit dem angegebenen Status „erneut verbunden“	`vserver cifs session file show -vserver vserver_name -reconnected {No

Es gibt weitere optionale Parameter, mit denen Sie die Ausgabeergebnisse verfeinern können. Weitere Informationen finden Sie auf der man-Seite.

Beispiele

Im folgenden Beispiel werden Informationen über offene Dateien auf SVM vs1 angezeigt:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

Im folgenden Beispiel werden ausführliche Informationen über offene SMB-Dateien mit der Datei-ID 82 auf

SVM vs1 angezeigt:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Verwandte Informationen

Anzeigen von SMB-Sitzungsinformationen

Ermitteln Sie, welche Statistikobjekte und Zähler verfügbar sind

Bevor Informationen über CIFS, SMB, Auditing und BranchCache Hash-Statistiken und die Performance überwacht werden können, müssen Unternehmen wissen, welche Objekte und Zähler verfügbar sind, von denen sie Daten beziehen können.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Sie können ermitteln, ob…	Eingeben…
Welche Objekte sind verfügbar	`statistics catalog object show`
Verfügbare spezifische Objekte	`statistics catalog object show object object_name`
Welche Zähler stehen zur Verfügung	`statistics catalog counter show object object_name`

Weitere Informationen darüber, welche Objekte und Zähler verfügbar sind, finden Sie auf den man-Pages.

3. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiele

Mit dem folgenden Befehl werden Beschreibungen ausgewählter Statistikobjekte angezeigt, die mit dem CIFS- und SMB-Zugriff im Cluster in Verbindung stehen, wie sie auf der erweiterten Berechtigungsebene angezeigt werden:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

Mit dem folgenden Befehl werden Informationen über einige der Zähler für die angezeigt `cifs` Objekt, wie auf der erweiterten Berechtigungsebene angezeigt:

> In diesem Beispiel werden nicht alle verfügbaren Zähler für das angezeigt `cifs` Objekt; Ausgabe wird abgeschnitten.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    ------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                             vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Verwandte Informationen

Anzeigen von Statistiken

Zeigen Sie Statistiken an

Sie können zur Überwachung der Performance und Diagnose von Problemen verschiedene Statistiken, darunter Statistiken zu CIFS und SMB, Audits und BranchCache-Hash, anzeigen.

Bevor Sie beginnen

Sie müssen Datenproben mithilfe des gesammelt haben `statistics start` Und `statistics stop` Befehle bevor Sie Informationen zu Objekten anzeigen können.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Statistiken anzeigen möchten für…	Eingeben…
Alle SMB-Versionen	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x und SMB 3.0	`statistics show -object smb2`
CIFS-Subsystem des Node	`statistics show -object nblade_cifs`
Multi-Protokoll-Prüfung	`statistics show -object audit_ng`
BranchCache-Hash-Service	`statistics show -object hashd`
Dynamisches DNS	`statistics show -object ddns_update`

   Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

3. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Verwandte Informationen

Ermitteln, welche Statistikobjekte und Zähler verfügbar sind

Überwachen der Statistiken von SMB-signierten Sitzungen

Anzeigen von BranchCache-Statistiken

Verwendung von Statistiken zur Überwachung der automatischen Knotenverweisungsaktivität

"SMB-Konfiguration für Microsoft Hyper-V und SQL Server"

"Einrichtung der Performance-Überwachung"

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.